Se manifiesta que el archivo publicado es la mejor versión disponible con la que cuenta el Instituto Mexicano del Seguro Social.

IMSS	**INSTITUTO MEXICANO DEL SEGURO SOCIAL** **DIRECCIÓN DE ADMINISTRACIÓN** **UNIDAD DE ADQUISICIONES E INFRAESTRUCTURA** **COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS** **COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS**	**Contrato Número** **P0M0026**

Contrato Abierto para la prestación del "Servicio de Continuidad de Nube IMSS 2020", que celebran por una parte, el **INSTITUTO MEXICANO DEL SEGURO SOCIAL**, que en lo sucesivo se denominará **"EL INSTITUTO"**, representado en este acto por el **C. ALBERTO FLAVIO BALDERAS HERNÁNDEZ**, en su carácter de Apoderado Legal, y por la otra parte, la empresa denominada **SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.**, a quien en lo sucesivo se le denominará **"EL PROVEEDOR"**, representada por el **C. JUAN CARLOS MARTÍNEZ VALDÉS**, en su carácter de Representante Legal, y a quienes en forma conjunta se les denominará **"LAS PARTES"**, al tenor de las Declaraciones y Cláusulas siguientes:

D E C L A R A C I O N E S

I.- "EL INSTITUTO" declara, a través de su Apoderado Legal que:

I.1.- Es un Organismo Descentralizado de la Administración Pública Federal con personalidad jurídica y patrimonio propios, que tiene a su cargo la organización y administración del Seguro Social, como un servicio público de carácter nacional, en términos de los artículos 4º y 5º de la Ley del Seguro Social.

I.2.- Está facultado para contratar los servicios necesarios, en términos de la legislación vigente, para la consecución de los fines para los que fue creado, de conformidad con el artículo 251, fracción IV de la Ley del Seguro Social.

I.3.- El C. Alberto Flavio Balderas Hernández, en su carácter de Titular de la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos, cuenta con las facultades suficientes para suscribir el presente instrumento jurídico en su calidad de Apoderado Legal, de conformidad con lo establecido en los artículos 268 A de la Ley de Seguro Social y 66 último párrafo del Reglamento Interior del Instituto Mexicano del Seguro Social, y acredita su personalidad mediante el testimonio de la Escritura Pública número 126,525 de fecha 15 de noviembre de 2019, otorgada ante la fe del Licenciado Eduardo García Villegas, Titular de la Notaría Pública número 15 de la Ciudad de México, e inscrita en el Registro Público de Organismos Descentralizados bajo el folio número 97-7-22112019-115904, de fecha 22 de noviembre de 2019, y manifiesta bajo protesta de decir verdad que las facultades que le fueron conferidas no le han sido revocadas, modificadas, ni restringidas en forma alguna en cumplimiento a los artículos 24 y 25 de la Ley Federal de las Entidades Paraestatales.

I.4.- El C. Eduardo Oropeza Ortíz, Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional de **"EL INSTITUTO"**, funge como Administrador del presente contrato, responsable de dar seguimiento y verificar el cumplimiento de los derechos y obligaciones establecidos en este instrumento jurídico, de conformidad con lo dispuesto en el artículo 84, penúltimo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

"Este Instrumento Jurídico fue elaborado de conformidad con los documentos correspondientes al procedimiento de contratación que se señala".

I.5.- Para el cumplimiento de sus funciones y la realización de sus actividades se requiere de la prestación del "Servicio de Continuidad de Nube IMSS 2020", solicitado por la Coordinación de Sistemas de Infraestructura Tecnológica Institucional.

I.6.- Para cubrir las erogaciones que se deriven del presente contrato, cuenta con los recursos disponibles suficientes, no comprometidos, en la cuenta número 42061506 de conformidad con el Dictamen de Disponibilidad Presupuestal Previo con número de folio 0000002003-2020, emitido por la Titular de la División de Control y Seguimiento al Gasto de Operación de fecha 30 de octubre de 2019, documento que se agrega al **Anexo 1 (uno)** del presente contrato.

I.7.- Con fecha 27 de diciembre de 2019, en la Sesión Extraordinaria número 15/2019, el Comité de Adquisiciones, Arrendamientos y Servicios (CAAS), dictaminó procedente el supuesto de excepción al procedimiento de Licitación Pública para llevar a cabo la contratación del Servicio de Continuidad de la Nube IMSS, para cubrir las necesidades de **"EL INSTITUTO"**, mediante Acuerdo número AC-39/SE-15/2019.

I.8.- Con fecha 30 de diciembre de 2019, la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos, a través de la División de Contratación de Activos y Logística, mediante acta de adjudicación, notificó a **"EL PROVEEDOR"** la adjudicación del procedimiento de Adjudicación Directa Nacional número **AA-050GYR019-E384-2019**, con fundamento en lo dispuesto en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos, 26 fracción III, 26 Bis fracción I, 28 fracción I, 40, 41 fracción III y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, los relativos de su Reglamento y demás disposiciones aplicables en la materia, como se detalla en el **Anexo 2 (dos)** del presente instrumento jurídico.

I.9.- De conformidad con lo previsto en el artículo 81, fracción IV del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en caso de discrepancia entre el contenido de la solicitud de cotización y el presente instrumento jurídico, prevalecerá lo establecido en dicha solicitud.

I.10.- Señala como su domicilio para todos los efectos de este acto jurídico, el ubicado en Calle Durango número 291, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, en la Ciudad de México.

II.- "EL PROVEEDOR" declara, a través de su Representante Legal, que:

II.1.- Es una persona moral constituida de conformidad con las leyes de los Estados Unidos Mexicanos, según consta en la Escritura Pública número 95,987 de fecha 23 de marzo de 2001, pasada ante la fe del Licenciado Arturo Sobrino Franco, Titular de la Notaría Pública número 49 del Distrito Federal, inscrita en el Registro Público de Comercio de la misma Entidad, en el folio mercantil número 275514.

II.2.- El C. Juan Carlos Martínez Valdés , acredita su personalidad en términos de la Escritura Pública número 77,500 de fecha 25 de agosto de 2016, pasada ante la fe del Licenciado Roberto Nuñez y Bandera, Titular de la Notaría Pública número 1 de la Ciudad de México, inscrita en el Registro Público de la Propiedad y de Comercio de la misma Entidad, en el folio mercantil número 275514*, y manifiesta bajo protesta de decir verdad que las facultades que le fueron conferidas no le han sido revocadas, modificadas, ni restringidas en forma alguna.

II.3.- Su objeto social conforme a sus Estatutos consiste, entre otros, en la prestación de servicios de "hosting" o alojamiento de páginas de Internet, incluyendo de manera enunciativa mas no limitativa, la adquisición, mantenimiento, instalación de, y prestación de servicios con, ordenadores de base de datos; monitoreo remoto de páginas de Internet los trescientos sesenta y cinco días del año; provisión de conectividad global de alta velocidad a las páginas de Internet de clientes; así como la aplicación de medidas de seguridad para evitar la invasión o la alteración del contenido de las páginas de Internet de los clientes de la sociedad.

II.4.- Cuenta con Registro Federal de Contribuyentes número: **SNM010323EB5**.

II.5.- Cuenta, al igual que su subcontratante, con el documento vigente expedido por el Servicio de Administración Tributaria (SAT), de opinión de cumplimiento de obligaciones fiscales en sentido positivo, de conformidad con el artículo 32 D del Código Fiscal de la Federación, así como a lo dispuesto por las Reglas 2.1.31 y 2.1.39 de la Resolución Miscelánea Fiscal para 2020, publicada el 28 de diciembre de 2019 en el Diario Oficial de la Federación, de los cuales presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

II.6.- Cuenta, al igual que su subcontratante, con el documento correspondiente vigente, expedido por **"EL INSTITUTO"** sobre el cumplimiento de sus obligaciones fiscales en materia de seguridad social, conforme al Acuerdo ACDO.SA1.HCT.101214/281.P.DIR dictado por el H. Consejo Técnico de **"EL INSTITUTO"** en la sesión ordinaria celebrada el 10 de diciembre de 2014, publicado en el Diario Oficial de la Federación el 27 de febrero de 2015 y su modificación publicada en el mismo de fecha 3 de abril de 2015, de los cuales presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

II.7.- Cuenta, al igual que su subcontratante, con el documento correspondiente vigente, expedido por el INFONAVIT en los términos del Acuerdo del H. Consejo de Administración del Instituto del Fondo Nacional de la Vivienda para los Trabajadores por el que se emiten las Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos, publicado en el Diario Oficial de la Federación el 28 de junio de 2017, de los cuales presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

II.8.- Manifiesta bajo protesta de decir verdad, no encontrarse en los supuestos de los artículos 50 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

En caso de que **"EL PROVEEDOR"** se encuentre en los supuestos señalados anteriormente, el contrato será nulo previa determinación de la autoridad competente de conformidad con lo establecido en el artículo 15 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

II.9.- Conforme a lo previsto en los artículos 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 107 de su Reglamento, **"EL PROVEEDOR"**, en caso de auditorías, visitas o inspecciones que practique la Secretaría de la Función Pública y el Órgano Interno de Control en **"EL INSTITUTO"**, deberá proporcionar la información relativa al presente contrato que en su momento se requiera.

II.10.- Reúne las condiciones de organización, experiencia, personal capacitado y demás recursos técnicos, humanos y económicos necesarios, así como con la capacidad legal suficiente para cumplir con las obligaciones que contrae en el presente contrato.

II.11.- Para efectos legales y de notificación relacionados con el presente contrato, señala como domicilio para oír y recibir toda clase de notificaciones y documentos, el ubicado en Prolongación Paseo de la Reforma número 5287, Colonia Cuajimalpa, Código Postal 05000, Demarcación Territorial Cuajimalpa de Morelos, en la Ciudad de México, teléfono: (55) 8503 2647 Ext. 5151, correo electrónico: cvaldes@kionetworks.com.

Hechas las declaraciones anteriores, **"LAS PARTES"** convienen en otorgar el presente contrato, de conformidad con las siguientes:

C L Á U S U L A S

PRIMERA.- OBJETO DEL CONTRATO.- "EL PROVEEDOR" se obliga a prestar el "Servicio de Continuidad de Nube IMSS 2020", cuyas características, cantidades, alcances y especificaciones se describen en los **Anexos 1 (uno)** y **2 (dos)** del presente instrumento jurídico, así como a las condiciones de la solicitud de cotización y acta de adjudicación del procedimiento del cual deriva el presente contrato.

SEGUNDA.- IMPORTE DEL CONTRATO.- El importe del presente contrato es por la cantidad mínima de **$252,092,911.77 (DOSCIENTOS CINCUENTA Y DOS MILLONES NOVENTA Y DOS MIL NOVECIENTOS ONCE PESOS 77/100 M.N.)**, incluye el Impuesto al Valor Agregado (I.V.A.), y por la cantidad máxima de **$630,232,279.43 (SEISCIENTOS TREINTA MILLONES DOSCIENTOS TREINTA Y DOS MIL DOSCIENTOS SETENTA Y NUEVE PESOS 43/100 M.N.)**, incluye el Impuesto al Valor Agregado (I.V.A.), de conformidad con los precios unitarios que se indican en el **Anexo 2 (dos)** del presente contrato.

"LAS PARTES" convienen que el presente contrato se celebra bajo la modalidad de precios fijos, de acuerdo con los precios unitarios pactados, por lo que el monto de los mismos no cambiará durante la vigencia del presente instrumento jurídico.

TERCERA.- FORMA Y CONDICIONES DE PAGO.- Se efectuará el pago a **"EL PROVEEDOR"** de manera "Mensual" para los servicios recurrentes, por "Evento" para los que sean solicitados a discreción de **"EL INSTITUTO"** y por "Única Ocasión", para los servicios que están planificados como única vez en la vida del contrato, de conformidad con lo dispuesto en el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como lo establecido en el Anexo Técnico, Apéndices y en los Términos y Condiciones que se agregan en el **Anexo 1 (uno)** del presente contrato.

"EL PROVEEDOR" reportará y solicitará a **"EL INSTITUTO"** el pago asociado a los servicios que haya entregado o que hayan sido consumidos, conforme a las especificaciones descritas en el Anexo Técnico integrado en el **Anexo 1 (uno)** del presente instrumento jurídico, con estricto apego a las características y niveles de servicio que se requieren para cada rubro definido en el catálogo de servicios, y que cumplan con los aspectos generales de su operación; sujeto a posibles deducciones por incumplimiento de los mismos, por lo que **"EL INSTITUTO"**, a través del Administrador del presente contrato, evaluará y dictaminará las condiciones de funcionalidad, operatividad y consumo de los servicios que sean prestados por **"EL PROVEEDOR"** para que proceda el pago mensual que debe efectuarse por los mismos.

"EL PROVEEDOR" deberá presentar ante el Administrador del contrato, la documentación comprobatoria (entregables) y Acta de Aceptación del Servicio, con la que acreditará fehacientemente que se ha proporcionado el servicio a entera satisfacción de **"EL INSTITUTO"**, y en estricto apego al procedimiento administrativo vigente en **"EL INSTITUTO"**. Dichos servicios deberán sustentarse mediante la entrega documental a **"EL INSTITUTO"**.

"EL PROVEEDOR" entregará oportunamente la representación impresa del Comprobante Fiscal Digital por Internet (CFDI) por los servicios del mes, en la Coordinación de Servicios Administrativos de la Dirección de Innovación y Desarrollo Tecnológico, así como la nota de crédito respectiva, en caso de que aplique, para que sean debidamente sancionadas, de acuerdo con los requisitos fiscales que establece el artículo 29-A del Código Fiscal de la Federación.

"EL PROVEEDOR" deberá generar los CFDI por períodos mensuales vencidos de servicio, y las entregará a **"EL INSTITUTO"** en los primeros diez días naturales del mes siguiente al que se factura, de acuerdo con lo siguiente:

a) **"EL PROVEEDOR"**entregará el CFDI a la Coordinación de Servicios Administrativos de la DIDT.
b) La Coordinación de Servicios Administrativos enviará el CFDI a la Coordinación de Sistemas de Infraestructura Tecnológica de **"EL INSTITUTO"** para su trámite en términos del contrato.
c) La Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI) enviará al Administrador del contrato, el CFDI con la petición de que proceda a la validación de los

servicios comprendidos en la misma, en su caso, emita la aceptación a entera satisfacción de los servicios.
d) El Administrador del Contrato integrará los respectivos sustentos documentales incluyendo los resultados del cálculo de las métricas de los niveles de servicio establecidos en el Anexo Técnico integrado en el **Anexo 1 (uno)** del presente instrumento jurídico, para la aplicación de deducciones y penas convencionales conducentes enviándola a la Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI).
e) La Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI) valida y enviará la documentación completa a la Coordinación de Servicios Administrativos para la gestión de pago.
f) La Coordinación de Servicios Administrativos entregará el CFDI a **"EL PROVEEDOR"**.
g) **"EL PROVEEDOR"** deberá ingresar su CFDI y documentación al área de Trámite de Erogaciones para los trámites correspondientes.

El pago se realizará en moneda nacional, en los plazos normados por la Dirección de Finanzas en el "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos", sin que éstos rebasen los 20 (veinte) días naturales posteriores a aquel en que **"EL PROVEEDOR"** presente en las oficinas de la División de Trámite de Erogaciones, sita en Calle Gobernador Tiburcio Montiel número 15 (esquina con Gómez Pedraza), Colonia San Miguel Chapultepec, Demarcación Territorial Miguel Hidalgo, Código Postal 11850, en la Ciudad de México, en días y horas hábiles, la documentación correspondiente para pago.

"EL PROVEEDOR" deberá entregar a **"EL INSTITUTO"** la "Opinión de cumplimiento de obligaciones en materia de seguridad social", vigente y positiva, junto con el CFDI de cobro respectivo mensual, así como entregar el documento vigente expedido por el SAT en el que se emita la opinión de cumplimiento de las obligaciones fiscales positivo y vigente.

"EL PROVEEDOR" deberá expedir sus CFDI, en el esquema de facturación electrónica, con las especificaciones normadas por el Servicio de Administración Tributaria (SAT) a nombre del Instituto Mexicano del Seguro Social, con Registro Federal de Contribuyentes IMS421231I45, domicilio en Avenida Paseo de la Reforma número 476, Colonia Juárez, Código Postal 06600, Demarcación Territorial Cuauhtémoc, en la Ciudad de México.

El CFDI deberá reunir los requisitos fiscales establecidos en la Ley de la materia, indicando los servicios prestados, así como el número de contrato. Una vez validada la documentación anterior y previo cotejo con la coordinación responsable, se procederá a la liberación del CFDI y documentación soporte de **"EL PROVEEDOR"**, para que éste la entregue ante la División de Trámite de Erogaciones.

"EL PROVEEDOR", para cada uno de los pagos que efectivamente reciba, de acuerdo con esta cláusula, deberá de expedir a nombre de **"EL INSTITUTO"**, el "CFDI con complemento para la recepción de pagos", también denominado "recibo electrónico de pago", el cual

elaborará dentro de los plazos establecidos por las disposiciones fiscales vigentes y lo cargará en el portal de servicios a proveedores de la página de **"EL INSTITUTO"**.

Para la validación de dichos comprobantes **"EL PROVEEDOR"** deberá cargar en internet, a través del portal de servicios a proveedores de la página de **"EL INSTITUTO"** el archivo en formato XML, la validez de los mismos será determinada durante la carga y únicamente los comprobantes válidos serán procedentes para pago.

El pago se realizará mediante transferencia electrónica de fondos, a través del esquema electrónico interbancario que **"EL INSTITUTO"** tiene en operación; para tal efecto, **"EL PROVEEDOR"** proporcionará con oportunidad su número de cuenta, CLABE, banco y sucursal, a menos que **"EL PROVEEDOR"** acredite en forma fehaciente la imposibilidad para ello.

El pago se depositará en la fecha programada, a través del esquema interbancario si la cuenta bancaria de **"EL PROVEEDOR"** está contratada con BANORTE, BBVA BANCOMER, HSBC, SCOTIABANK INVERLAT o a través del esquema interbancario vía SPEI (Sistema de Pagos Electrónicos Interbancarios), si la cuenta pertenece a un banco distinto a los antes mencionados.

El administrador del contrato será quien dará la autorización para que la Dirección de Finanzas proceda a su pago de acuerdo con lo normado en el anexo "Cuentas Contables" del "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos".

En ningún caso se deberá autorizar el pago del servicio, sí no se ha determinado, calculado y notificado a **"EL PROVEEDOR"** las penas convencionales o deducciones pactadas en el presente contrato, así como su registro y validación en el Sistema PREI Millenium.

"EL PROVEEDOR" se obliga a no cancelar ante el SAT los CFDI a favor de **"EL INSTITUTO"** previamente validados en el portal de servicios a proveedores, salvo justificación y comunicación por parte del mismo al administrador del contrato para su autorización expresa, debiendo éste informar a las áreas de trámite de erogaciones de dicha justificación y reposición del CFDI en su caso.

"EL PROVEEDOR" deberá entregar el CFDI a favor de **"EL INSTITUTO"** por el importe de la aplicación de la pena convencional por atraso.

Las Unidades Responsables del Gasto (URG) deberán registrar el contrato y su dictamen presupuestal en el Sistema PREI Millenium para el trámite de pago correspondiente.

"EL PROVEEDOR", durante la vigencia del presente contrato, se obliga a presentar a **"EL INSTITUTO"**, junto con el CFDI respectivo la constancia positiva y vigente emitida por el

INFONAVIT y la "Opinión de cumplimiento de obligaciones en materia de seguridad social", vigente y positiva, la cual puede ser consultada a través de la página electrónica http://www.imss.gob.mx/tramites/cumplimiento-obligaciones, en los términos requeridos por **"EL INSTITUTO"**.

Los servicios cuya recepción no genere alta a través del SAI ni realice al PREI Millenium de manera electrónica, deberán contener la firma de recepción y de autorización para el trámite de pago de acuerdo a lo establecido en el "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos" vigente, así como el Acta de Entrega-Recepción.

Para que **"EL PROVEEDOR"** pueda celebrar un contrato de cesión de derechos de cobro, deberá notificarlo por escrito a **"EL INSTITUTO"** con un mínimo de 5 días naturales anteriores a la fecha de pago programada; el Administrador del Contrato o, en su caso, el Titular del Área Requirente, deberá entregar los documentos sustantivos de dicha cesión al área responsable de realizar el proceso, conforme al "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos".

De igual forma procederá en caso de que celebre contrato de cesión de derechos de cobro a través de factoraje financiero conforme al Programa de Cadenas Productivas de Nacional Financiera, S.N.C., Institución de Banca de Desarrollo.

En caso de que **"EL PROVEEDOR"** reciba pagos en exceso deberá reintegrar las cantidades pagadas en exceso más los intereses correspondientes, conforme a la tasa que establezca la Ley de Ingresos de la Federación, en los casos de prórroga para el pago de créditos fiscales. Los intereses se calcularán sobre las cantidades en exceso y se computarán por días naturales desde la fecha de su entrega hasta la fecha en que se pongan efectivamente las cantidades a disposición de **"EL INSTITUTO"**.

En caso de que **"EL PROVEEDOR"** presente su CFDI con errores o deficiencias, conforme a lo previsto en los artículos 89 y 90 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"EL INSTITUTO"** dentro de los 3 (tres) días hábiles siguientes a la recepción de la misma, indicará por escrito a **"EL PROVEEDOR"** las deficiencias o errores que deberá corregir. El periodo que transcurra a partir de la entrega del citado escrito y hasta que **"EL PROVEEDOR"** presente las correcciones no se computará dentro del plazo estipulado para el pago.

El Administrador del Contrato llevará a cabo la valoración de la procedencia del pago por concepto de gastos no recuperables conforme a lo previsto en los artículos 101 y 102 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en relación con los artículos 38, 46, 54 Bis y 55 Bis, segundo párrafo de la Ley de Adquisiciones,

Arrendamientos y Servicios del Sector Público, previa solicitud por escrito a **"EL PROVEEDOR"**, acompañada de los documentos siguientes:

• Copia de la identificación oficial vigente con fotografía y firma de la persona que haya realizado los trámites relacionados con el procedimiento de contratación.

• El CFDI que reúna los requisitos de los artículos 29 y 29-A del CFF, 37 al 40 del RCFF y, en su caso, la Resolución de la Miscelánea Fiscal del Ejercicio que corresponda.

• La solicitud la realizará al Administrador del Contrato para la determinación de la procedencia del pago y, en su caso, elaborar el finiquito y remitirlo para el pago respectivo a la Coordinación de Contabilidad y Trámite de Erogaciones, dependiente de la Dirección de Finanzas.

El pago del servicio quedará condicionado proporcionalmente al pago que **"EL PROVEEDOR"** deba efectuar por concepto de penas convencionales por atraso y/o por concepto de deducciones. En ambos casos, **"EL INSTITUTO"** realizará las retenciones correspondientes sobre el CFDI que se presente para pago. En el entendido de que en el supuesto de que sea rescindido el contrato, no procederá el cobro de dichas penalizaciones, ni la contabilización de las mismas para hacer efectiva la garantía de cumplimiento, de conformidad con lo establecido por el artículo 95 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

CUARTA.- PLAZO, LUGAR Y CONDICIONES DE LA PRESTACIÓN DEL SERVICIO.- "EL PROVEEDOR" se obliga a prestar a **"EL INSTITUTO"** el servicio que se menciona en la Cláusula Primera del presente instrumento jurídico, conforme a lo establecido en el Anexo Técnico y en los Términos y Condiciones integrados en el **Anexo 1 (uno)** de este contrato, apegándose a las condiciones, alcances y características detalladas en la solicitud de cotización y acta de adjudicación del procedimiento del cual deriva el presente contrato, y de acuerdo con lo siguiente:

PLAZO DE LA PRESTACIÓN DEL SERVICIO.- Será a partir del día hábil siguiente de la notificación del Acta de Adjudicación y hasta el 31 de diciembre de 2020.

Lo anterior de conformidad con los artículos 46 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 84 de su Reglamento.

LUGAR DE LA PRESTACIÓN DEL SERVICIO.- "EL PROVEEDOR" se obliga expresamente a prestar el servicio en los lugares señalados en el Anexo Técnico, Apéndices y en los Términos y Condiciones, integrados en el **Anexo 1 (uno)** de este contrato o en las nuevas ubicaciones que **"EL INSTITUTO"** defina durante la vigencia del presente contrato, ya sea incrementando o sustituyendo alguna de las ubicaciones existentes, con objeto de acondicionar los servicios necesarios para su adecuado funcionamiento.

CONDICIONES DE LA PRESTACIÓN DEL SERVICIO.- "EL PROVEEDOR" se obliga con **"EL INSTITUTO"** a cumplir con las condiciones del servicio adquiridas, de acuerdo a lo establecido en el Anexo Técnico, Apendices y en los Términos y Condiciones que se integran en el presente contrato como **Anexo 1 (uno)**, así como a lo ofrecido en sus propuestas técnica y económica que se agregan en el **Anexo 2 (dos)**.

Cabe resaltar que mientras no se cumpla con las condiciones de la prestación del servicio establecidas, **"EL INSTITUTO"** no dará por aceptado el servicio objeto de este contrato.

QUINTA.- VIGENCIA.- "LAS PARTES" convienen que la vigencia del presente contrato será a partir del día hábil siguiente de la notificación del Acta de Adjudicación y hasta el 31 de diciembre de 2020.

SEXTA.- TRANSFERENCIA DE DERECHOS DE COBRO.- "EL PROVEEDOR" se obliga a no transferir o ceder por ningún título, en forma total o parcial, a favor de cualquier otra persona física o moral, sus derechos y obligaciones que se deriven del presente contrato; a excepción de los derechos de cobro, debiendo, en este caso, solicitar por escrito el consentimiento de **"EL INSTITUTO"** a través del administrador del presente contrato para tal efecto.

"EL PROVEEDOR" deberá presentar la solicitud correspondiente dentro de los 5 (cinco) días naturales anteriores a la fecha de pago programada, a la que deberá adjuntar una copia de los contra-recibos cuyo importe transfiere, y demás documentos sustantivos de dicha transferencia, lo cual será necesario para efectuar el pago correspondiente.

Si con motivo de la transferencia de los derechos de cobro solicitada por **"EL PROVEEDOR"** se origina un retraso en el pago, no procederá el pago de los gastos financieros a que hace referencia el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

SÉPTIMA.- RESPONSABILIDAD.- Conforme a lo previsto en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"EL PROVEEDOR"** se obliga a responder por su cuenta y riesgo de los daños y/o perjuicios que por inobservancia o negligencia de su parte, llegue a causar a **"EL INSTITUTO"** y/o a terceros. Asimismo, se obliga a cumplir cabalmente el objeto del presente contrato y a entera satisfacción de **"EL INSTITUTO"**; por lo que responderá de los defectos y vicios ocultos que afecten la calidad de los servicios entregados, tanto durante el tiempo de vigencia de este contrato como durante la vida útil del bien, así como a responder de cualquier otra responsabilidad en que hubiere incurrido en los términos señalados en el Código Civil Federal.

Lo anterior, de acuerdo a la Garantía del Servicio descrita en la Cláusula Décima, inciso a), del presente contrato.

OCTAVA.- CONTRIBUCIONES.- Los impuestos y/o derechos que procedan con motivo del servicio objeto del presente contrato, serán pagados por **"EL PROVEEDOR"** conforme a la legislación aplicable en la materia.

"EL INSTITUTO" sólo cubrirá el Impuesto al Valor Agregado (I.V.A.), de acuerdo con lo establecido en las disposiciones fiscales vigentes en la materia.

"EL PROVEEDOR", en su caso, cumplirá con la inscripción de sus trabajadores en el régimen obligatorio del Seguro Social, así como con el pago de las cuotas obrero-patronales a que haya lugar, conforme a lo dispuesto en la Ley del Seguro Social. **"EL INSTITUTO"**, a través del Área fiscalizadora competente, podrá verificar en cualquier momento el cumplimiento de dicha obligación.

"EL PROVEEDOR" que tenga cuentas líquidas y exigibles a su cargo por concepto de cuotas obrero patronales, conforme a lo previsto en el artículo 40 B de la Ley del Seguro Social, acepta que **"EL INSTITUTO"** las compense con el o los pagos que tenga que hacerle por concepto de contraprestación por la contratación del servicio.

NOVENA.- PROPIEDAD INTELECTUAL, PATENTES Y/O MARCAS.- "EL PROVEEDOR" se obliga para con **"EL INSTITUTO"**, a responder por los daños y/o perjuicios que pudiera causar a **"EL INSTITUTO"** y/o a terceros, si con motivo de la prestación del servicio se violan derechos de autor, de patentes y/o marcas u otro derecho reservado a nivel Nacional o Internacional.

Por lo anterior, **"EL PROVEEDOR"** manifiesta en este acto bajo protesta de decir verdad, no encontrarse en ninguno de los supuestos de infracción a la Ley Federal del Derecho de Autor, ni a la Ley de la Propiedad Industrial.

En caso de que sobreviniera alguna reclamación en contra de **"EL INSTITUTO"** por cualquiera de las causas antes mencionadas, la única obligación de éste será la de dar aviso en el domicilio previsto en este instrumento jurídico a **"EL PROVEEDOR"**, para que éste lleve a cabo las acciones necesarias que garanticen la liberación de **"EL INSTITUTO"** de cualquier controversia o responsabilidad de carácter civil, mercantil, penal o administrativa que, en su caso, se ocasione.

Lo anterior de conformidad a lo establecido en el artículo 45, fracción XX de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Asimismo, se deberá observar lo establecido en los numerales 7 y 9 de los Términos y Condiciones, que se agregan en el **Anexo 1 (uno)** del presente contrato.

DÉCIMA.- GARANTÍAS.- "EL PROVEEDOR" se obliga a entregar a **"EL INSTITUTO"** las garantías que a continuación se indican:

a) **DEL SERVICIO.- "EL PROVEEDOR"** presenta en su propuesta técnica la documentación necesaria para garantizar el soporte de los fabricantes involucrados en la provisión de sus servicios; a fin de lograr los Niveles de Servicio requeridos en el Anexo Técnico, integrado en el **Anexo 1 (uno)** de este contrato.

b) **DE CUMPLIMIENTO DEL CONTRATO.- "EL PROVEEDOR"** se obliga a entregar a más tardar dentro de los 10 (diez) días naturales posteriores a la firma de este instrumento jurídico, en términos de la fracción II del artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, una garantía de cumplimiento de todas y cada una de las obligaciones a su cargo derivadas del presente contrato, mediante fianza expedida por compañía autorizada en los términos de la Ley de Instituciones de Seguros y de Fianzas a favor del "Instituto Mexicano del Seguro Social" por un monto equivalente al 20% (veinte por ciento) sobre el importe máximo que se indica en la Cláusula Segunda del presente contrato, sin considerar el Impuesto al Valor Agregado (I.V.A.) y/o IEPS, según sea el caso, en Moneda Nacional.

"EL PROVEEDOR" queda obligado a entregar a **"EL INSTITUTO"** la póliza de fianza antes señalada, en la División de Contratos, ubicada en Calle Durango número 291, 10° piso, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, en la Ciudad de México, apegándose al formato que para tal efecto se entregará en la referida División.

Dicha póliza de garantía de cumplimiento del contrato se liberará de forma inmediata a **"EL PROVEEDOR"** una vez que **"EL INSTITUTO"** le otorgue autorización por escrito, para que éste pueda solicitar a la afianzadora correspondiente la cancelación de la fianza, autorización que se entregará a **"EL PROVEEDOR"** siempre que demuestre haber cumplido con la totalidad de las obligaciones adquiridas por virtud del presente contrato; para lo anterior, deberá presentar mediante escrito la solicitud de liberación de la fianza en la División de Contratos, misma que llevará a cabo el procedimiento para su liberación y entrega.

ENDOSO DE LA GARANTÍA DE CUMPLIMIENTO.- En el supuesto de que **"EL INSTITUTO"** y por así convenir a sus intereses, decidiera modificar en cualquiera de sus partes el presente contrato**, "EL PROVEEDOR"** se obliga a otorgar el endoso de la póliza de garantía originalmente entregada, en el que conste las modificaciones o cambios en la respectiva fianza, observándose los mismos términos y condiciones señalados en la presente cláusula para la entrega de la garantía de cumplimiento, debiéndola entregar **"EL PROVEEDOR"** a más tardar dentro de los 10 (diez) días naturales posteriores a la firma del convenio respectivo.

DÉCIMA PRIMERA.- EJECUCIÓN DE LA GARANTÍA DE CUMPLIMIENTO DE ESTE CONTRATO.- "EL INSTITUTO" llevará a cabo la ejecución de la garantía de cumplimiento de contrato en los casos siguientes:

a) Se rescinda administrativamente el presente contrato.

b) Durante su vigencia se detecten deficiencias, fallas o calidad inferior del servicio prestado, en comparación con lo ofertado.

c) Cuando en el supuesto de que se realicen modificaciones al contrato, **"EL PROVEEDOR"** no entregue en el plazo pactado el endoso o la nueva garantía, que ampare el porcentaje establecido para garantizar el cumplimiento del presente instrumento, de conformidad con la cláusula Décima, inciso b).

d) Por cualquier otro incumplimiento de las obligaciones contraídas en este contrato.

De conformidad con el artículo 81, fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, la aplicación de la garantía de cumplimiento se hará efectiva de manera proporcional al monto de las obligaciones incumplidas.

DÉCIMA SEGUNDA.- PENAS CONVENCIONALES.- De conformidad con lo establecido en los artículos 45, fracción XIX, 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 95 y 96 de su Reglamento, la pena convencional aplicable a **"EL PROVEEDOR"**, por atraso en el cumplimiento de la prestación del servicio será conforme a lo señalado en los Términos y Condiciones, Anexo Técnico y de acuerdo a los porcentajes y conceptos señalados en el Apéndice número 6 denominado Métricas de Niveles de Servicio del Anexo Técnico, documentos incluidos en el **Anexo 1 (uno)** del presente contrato.

El Administrador del presente contrato será el responsable de determinar, calcular y aplicar las penas convencionales, vigilando los correspondientes registro o captura y validación en el sistema PREI Millenium, así como de notificarlas a **"EL PROVEEDOR"** personalmente, mediante oficio o por medios de comunicación electrónica.

"EL INSTITUTO" descontará las cantidades que resulten de aplicar la pena convencional, sobre los pagos que deba cubrir a **"EL PROVEEDOR"**. Por lo tanto, **"EL PROVEEDOR"** autoriza a descontar las cantidades que resulten de aplicar las sanciones señaladas en párrafos anteriores, sobre los pagos que éste deba cubrirle a **"EL INSTITUTO"** durante el período en que incurra y/o se mantenga en atraso con motivo de la prestación del servicio.

Para autorizar el pago del servicio, previamente **"EL PROVEEDOR"** tiene que haber cubierto las penas convencionales aplicadas conforme a lo dispuesto en el presente contrato. El administrador del presente contrato será el responsable de verificar que se cumpla esta obligación, dentro de los 5 (cinco) días hábiles siguientes a la conclusión del atraso.

DÉCIMA TERCERA.- DEDUCCIONES.- Con fundamento en lo dispuesto en los artículos 53 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 97 de su Reglamento, **"EL PROVEEDOR"**, con motivo del incumplimiento parcial o deficiente de los servicios, se hará acreedor a una sanción conforme a los porcentajes y conceptos señalados en los Términos y Condiciones, Anexo Técnico y el Apéndice número 6 denominado Métricas

de Niveles de Servicio del Anexo Técnico, documentos incluidos en el **Anexo 1 (uno)** del presente contrato.

El administrador del presente contrato será responsable del cálculo, aplicación y seguimiento de las deducciones. El monto máximo de aplicación de las deducciones no podrán ser mayor al que resulte de aplicar el porcentaje de la garantía de cumplimiento del presente contrato.

DÉCIMA CUARTA.- TERMINACIÓN ANTICIPADA DEL CONTRATO.- De conformidad con lo establecido en el artículo 54 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 102 de su Reglamento, **"EL INSTITUTO"** podrá dar por terminado anticipadamente el presente contrato sin responsabilidad para éste y sin necesidad de que medie resolución judicial alguna, cuando concurran razones de interés general o bien cuando por causas justificadas se extinga la necesidad de requerir el servicio, objeto del presente contrato, y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas se ocasionaría algún daño o perjuicio a **"EL INSTITUTO"** o se determine la nulidad de los actos que dieron origen al presente instrumento jurídico, con motivo de la resolución de una inconformidad o intervención de oficio emitida por la Secretaría de la Función Pública.

La terminación anticipada del presente contrato se sustentará mediante dictamen que precise las razones o las causas justificadas que den origen a la misma. Los gastos no recuperables por la terminación anticipada serán pagados siempre que éstos sean razonables, estén comprobados y se relacionen directamente con el presente instrumento jurídico.

DÉCIMA QUINTA.- SUSPENSIÓN DEL SERVICIO.- En caso fortuito o fuerza mayor, bajo su responsabilidad, **"EL INSTITUTO"** podrá suspender la prestación del servicio en términos del artículo 55 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en cuyo caso únicamente se pagarán aquéllos que hubiesen sido efectivamente prestados.

Cuando la suspensión obedezca a causas imputables a **"EL INSTITUTO"**, se pagarán previa solicitud de **"EL PROVEEDOR"** los gastos no recuperables de conformidad con el artículo 102, fracción II, del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, para lo cual deberá presentar su solicitud a **"EL INSTITUTO"** para su revisión y validación, una relación pormenorizada de los gastos, los cuales deberán estar debidamente justificados, sean razonables, se relacionen directamente con el objeto del servicio contratado y a entera satisfacción del administrador del presente contrato.

DÉCIMA SEXTA.- CAUSALES DE RESCISIÓN ADMINISTRATIVA DEL CONTRATO.- "EL INSTITUTO" podrá rescindir administrativamente este contrato sin más responsabilidad para el mismo y sin necesidad de resolución judicial, cuando **"EL PROVEEDOR"** incurra en cualquiera de las causales que se señalan a continuación:

1. Cuando no entregue la garantía de cumplimiento del presente contrato, a más tardar dentro de los 10 (diez) días naturales posteriores a la firma del mismo.

2. Cuando incurra en falta de veracidad total o parcial respecto a la información proporcionada para la celebración del presente contrato.
3. Cuando incumpla, total o parcialmente, con cualesquiera de las obligaciones establecidas en el presente contrato y sus anexos.
4. Cuando se compruebe que el servicio ha sido prestado con alcances y características distintas a las pactadas.
5. Cuando se transmitan total o parcialmente, bajo cualquier título y a favor de otra persona física o moral, los derechos y obligaciones a que se refiere el presente documento, con excepción de los derechos de cobro, previa autorización de **"EL INSTITUTO"**.
6. Si la autoridad competente declara el concurso mercantil o cualquier situación análoga o equivalente que afecte el patrimonio de **"EL PROVEEDOR"**.
7. Cuando de manera reiterativa y constante, **"EL PROVEEDOR"** sea sancionado por parte de **"EL INSTITUTO"** con penalizaciones y/o deducciones sobre el mismo concepto de los servicios que proporciona, o por ubicarse en los límites de incumplimientos previstos en la cláusula de penas convencionales y/o deducciones del presente instrumento.
8. Cuando se sitúe en alguno de los supuestos previstos en el artículo 50 de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público.
9. Si **"EL PROVEEDOR"** no permite a **"EL INSTITUTO"** la administración y verificación a que se refiere la cláusula correspondiente del presente contrato.

DÉCIMA SÉPTIMA.- RESCISIÓN ADMINISTRATIVA DEL CONTRATO.- "EL INSTITUTO", en términos de lo dispuesto en el artículo 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, podrá rescindir administrativamente el presente contrato en cualquier momento, cuando **"EL PROVEEDOR"** incurra en incumplimiento de cualquiera de las obligaciones a su cargo, de conformidad con el procedimiento siguiente:

a) Si **"EL INSTITUTO"** considera que **"EL PROVEEDOR"** ha incurrido en alguna de las causales de rescisión que se consignan en la Cláusula que antecede, lo hará saber a **"EL PROVEEDOR"** de forma indubitable por escrito, a efecto de que éste exponga lo que a su derecho convenga y aporte, en su caso, las pruebas que estime pertinentes, en un término de 5 (cinco) días hábiles, a partir de la notificación de la comunicación de referencia.

b) Transcurrido el término a que se refiere el inciso anterior, se resolverá considerando los argumentos y pruebas que hubiere hecho valer.

c) La determinación de dar o no por rescindido administrativamente el presente contrato, deberá ser debidamente fundada, motivada y comunicada por escrito a **"EL**

PROVEEDOR" dentro de los 15 (quince) días hábiles siguientes, al vencimiento del plazo señalado en el inciso a), de esta Cláusula.

En el supuesto de que se rescinda este contrato, **"EL INSTITUTO"** no aplicarán las penas convencionales, ni su contabilización para hacer efectiva la garantía de cumplimiento de este instrumento jurídico.

En caso de que **"EL INSTITUTO"** determine dar por rescindido el presente contrato, se deberá formular y notificar un finiquito dentro de los 20 (veinte) días naturales siguientes a la fecha en que se notifique la rescisión, de conformidad con el artículo 99 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en el que se hagan constar los pagos que, en su caso, deba efectuar **"EL INSTITUTO"** por concepto de la prestación del servicio por **"EL PROVEEDOR"** hasta el momento en que se determine la rescisión administrativa.

Iniciado un procedimiento de conciliación **"EL INSTITUTO"**, bajo su responsabilidad, podrá suspender el trámite del procedimiento de rescisión.

Si previamente a la determinación de dar por rescindido este contrato, **"EL PROVEEDOR"** presta el servicio, el procedimiento iniciado quedará sin efectos, previa aceptación y verificación de **"EL INSTITUTO"** por escrito, de que continúa vigente la necesidad de contar con el servicio y aplicando, en su caso, las penas convencionales correspondientes.

"EL INSTITUTO" podrá determinar no dar por rescindido este contrato, cuando durante el procedimiento advierta que dicha rescisión pudiera ocasionar algún daño o afectación a las funciones que tiene encomendadas. En este supuesto, **"EL INSTITUTO"** elaborará un dictamen en el cual justifique que los impactos económicos o de operación que se ocasionarían con la rescisión del contrato resultarían más inconvenientes.

De no darse por rescindido este contrato, **"EL INSTITUTO"** establecerá, con **"EL PROVEEDOR"**, un nuevo plazo para el cumplimiento de aquellas obligaciones que se hubiesen dejado de cumplir, a efecto de que **"EL PROVEEDOR"** subsane el incumplimiento que hubiere motivado el inicio del procedimiento de rescisión. Lo anterior se llevará a cabo a través de un convenio modificatorio en el que se atenderá a las condiciones previstas en los dos últimos párrafos del artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

DÉCIMA OCTAVA.- CONFIDENCIALIDAD.- "EL PROVEEDOR" entregará a **"EL INSTITUTO"** en un plazo no mayor a 05 (cinco) días naturales al acto de adjudicación, una carta de confidencialidad mediante el cual **"EL PROVEEDOR"** se obliga a no revelar, transferir, compartir ni ceder ningún dato o información de carácter sensible y confidencial que se hayan compartido entre **"EL PROVEEDOR"** y **"EL INSTITUTO"**.

"LAS PARTES" convienen considerar como confidencial todos los datos contenidos en: cintas magnéticas, programas de cómputo, disquetes o cualquier otro material que contenga información jurídica, operativa, técnica, financiera o de análisis, registros, documentos, especificaciones, productos, informes, dictámenes y desarrollos a que tenga acceso o que le sean proporcionados por **"EL INSTITUTO"**.

De igual forma, será considerada como confidencial aquella información proporcionada por **"EL INSTITUTO"** para la ejecución del servicio que preste **"EL PROVEEDOR"** y sea propiedad exclusiva de **"EL INSTITUTO"**.

Por lo anterior, **"EL PROVEEDOR"** reconoce que queda prohibida su difusión total o parcial en su favor o de terceros ajenos a la relación contractual, por cualquier medio, entre otros de manera enunciativa más no limitativa: vía oral, impresa, electrónica, magnética, y en general por ningún medio, conforme el plazo señalado en el artículo 15 de Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

En este sentido, **"EL PROVEEDOR"** acepta que la prohibición señalada en el párrafo anterior, comprende inclusive, en forma enunciativa, que no se podrá llevar a cabo la difusión de la informacion de **"EL INSTITUTO"** con fines de lucro, comerciales, académicos, educativos o para cualquier otro ajeno al objeto de la presente contratación, por lo que **"EL PROVEEDOR"** se responsabiliza del uso y cuidado de la información.

Por lo expuesto, **"EL PROVEEDOR"** se obliga a lo siguiente:

1. Mantener absoluta confidencialidad de la información a la cual tenga acceso, siendo responsable de que cada uno de los integrantes del personal asignado para el desarrollo y operación del proyecto, respetará el manejo correcto de la información.
2. Toda la información a que tenga acceso el personal que **"EL PROVEEDOR"** designe para la prestación de los servicios materia del presente contrato, es considerada de carácter confidencial, por lo que **"EL PROVEEDOR"** deberá garantizar que por ningún motivo se viole ninguno de los siguientes acuerdos:

    a. La información del **"EL INSTITUTO"** y a la cual tenga acceso el personal de **"EL PROVEEDOR"**, no deberá ser copiada o respaldada en ninguno de los equipos del personal de **"EL PROVEEDOR"**, sin autorización previa del Administrador del contrato dentro del ámbito de su competencia.
    b. El acceso a la información de **"EL INSTITUTO"** sólo podrá ser por personal de **"EL PROVEEDOR"**, sólo podrá ser por parte del personal autorizado por el Administrador del contrato dentro del ámbito de su competencia.
    c. De no cumplir con alguna de estas premisas, se considerará como una falta al acuerdo de confidencialidad que aceptó **"EL PROVEEDOR"**.

Cualquier persona que tuviera acceso a dicha información deberá ser advertida de lo convenido en este contrato, comprometiéndose a observar y cumplir lo acordado.

"LAS PARTES" convienen en que no será considerada como sujeta a las obligaciones de confidencialidad la siguiente documentación o información:

a) Aquella que sea conocida públicamente.
b) La que haya sido puesta a disposición de **"LAS PARTES"** por un tercero, antes de la fecha de celebración del contrato en forma confidencial.
c) La que haya sido desarrollada independientemente o adquirida por cualquiera de las partes, sin violar las estipulaciones del contrato o la que genere o desarrolle **"EL PROVEEDOR"** en sus centros de desarrollo.
d) Aquella cuya revelación haya sido aprobada previamente por escrito.
e) La que de acuerdo a la Ley u orden judicial o administrativa, deba ser suministrada a terceras personas.

El uso de la información confidencial no otorgará a ninguna de **"LAS PARTES"** la titularidad o derechos de autor de la otra.

DÉCIMA NOVENA.- RELACIÓN LABORAL.- "LAS PARTES" convienen en que **"EL INSTITUTO"** no adquiere ninguna obligación de carácter laboral para con **"EL PROVEEDOR"** ni para con los trabajadores que el mismo contrate para la realización del objeto del presente instrumento jurídico, toda vez que dicho personal depende exclusivamente de **"EL PROVEEDOR"**.

Por lo anterior, no se le considerará a **"EL INSTITUTO"** como patrón, ni aún substituto, y **"EL PROVEEDOR"** expresamente lo exime de cualquier responsabilidad de carácter civil, fiscal, de seguridad social, laboral o de otra especie, que en su caso pudiera llegar a generarse.

"EL PROVEEDOR" se obliga a liberar a **"EL INSTITUTO"** de cualquier reclamación de índole laboral o de seguridad social que sea presentada por parte de sus trabajadores, ante las autoridades competentes.

VIGÉSIMA.- MODIFICACIONES.- De conformidad con lo establecido en el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"EL INSTITUTO"** podrá celebrar por escrito Convenio Modificatorio, al presente contrato dentro de la vigencia del mismo. Para tal efecto, **"EL PROVEEDOR"** se obliga a entregar, en su caso, la modificación de la garantía, en términos del artículo 103, fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

PRÓRROGAS.- Asimismo, se podrán acordar prórrogas al plazo originalmente pactado por caso fortuito, fuerza mayor o por causas atribuibles a **"EL INSTITUTO"**, lo cual deberá estar debidamente acreditado en el expediente de contratación respectivo. **"EL PROVEEDOR"**

puede solicitar la modificación del plazo originalmente pactado cuando se actualicen y se acrediten los supuestos de caso fortuito o de fuerza mayor.

Cualquier modificación a los derechos y obligaciones estipuladas por **"LAS PARTES"** en el presente contrato, deberá formalizarse mediante convenio y por escrito, mismo que será suscrito por los servidores públicos que lo hayan hecho en el contrato, quienes los sustituyan o estén facultados para ello.

VIGÉSIMA PRIMERA.- ADMINISTRACIÓN Y VERIFICACIÓN.- El C. Eduardo Oropeza Ortíz, Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional de **"EL INSTITUTO"**, funge como Administrador del contrato, responsable de administrar y verificar su cumplimiento, de conformidad con lo establecido en el documento de designación de administrador del contrato que se agrega al presente como **Anexo 3 (tres)** y el artículo 84 penúltimo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

En el caso de que se lleve a cabo un relevo institucional temporal o permanente con dicho servidor público de **"EL INSTITUTO"** tendrá carácter de ADMINISTRADOR DEL CONTRATO la persona que sustituya al servidor público en el cargo, conforme a la designación correspondiente.

VIGÉSIMA SEGUNDA.- PROCEDIMIENTO DE CONCILIACIÓN.- En cualquier momento durante la vigencia del presente Contrato, **"EL PROVEEDOR"** o **"EL INSTITUTO"** podrán presentar ante el Órgano Interno de Control en **"EL INSTITUTO"** solicitud de conciliación por desavenencias, derivadas del presente instrumento jurídico, conforme a lo dispuesto por los artículos 77 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 128 de su Reglamento.

VIGÉSIMA TERCERA.- RELACIÓN DE ANEXOS.- Los anexos que se relacionan a continuación forman parte integrante del presente contrato.

Anexo 1 (uno)	"Dictamen de Disponibilidad Presupuestal Previo, Anexo Técnico, Apéndices y Términos y Condiciones"
Anexo 2 (dos)	"Propuesta Técnica, Propuesta Económica y Acta de Adjudicación"
Anexo 3 (tres)	"Documento de designación de Administrador del Contrato"

VIGÉSIMA CUARTA.- LEGISLACIÓN APLICABLE.- "LAS PARTES" se obligan a sujetarse estrictamente para el cumplimiento del presente contrato, a todas y cada una de las cláusulas del mismo, así como a lo establecido en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento y supletoriamente al Código Civil Federal, a la Ley Federal de Procedimiento Administrativo, al Código Federal de Procedimientos Civiles y demás ordenamientos aplicables en la materia.

"Este Instrumento Jurídico fue elaborado de conformidad con los documentos correspondientes al procedimiento de contratación que se señala".

VIGÉSIMA QUINTA.- JURISDICCIÓN.- Para la interpretación y cumplimiento de este instrumento jurídico, así como para todo aquello que no esté expresamente estipulado en el mismo, **"LAS PARTES"** se someten a la jurisdicción de los Tribunales Federales competentes de la Ciudad de México, renunciando a cualquier otro fuero presente o futuro que por razón de su domicilio les pudiera corresponder.

Previa lectura y debidamente enteradas **"LAS PARTES"** del contenido, alcance y fuerza legal del presente contrato, en virtud de que se ajusta a la expresión de su libre voluntad y que su consentimiento no se encuentra afectado por dolo, error, mala fe, ni otros vicios de la voluntad, lo firman y ratifican en todas sus partes, por quintuplicado, en la Ciudad de México, el **15 de enero de 2020**, quedando un ejemplar en poder de **"EL PROVEEDOR"** y los restantes en poder de **"EL INSTITUTO"**.

"EL INSTITUTO" INSTITUTO MEXICANO DEL SEGURO SOCIAL	"EL PROVEEDOR" SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.
C. ALBERTO FLAVIO BALDERAS HERNÁNDEZ Apoderado Legal	**C. JUAN CARLOS MARTÍNEZ VALDÉS** Representante Legal

ADMINISTRADOR DEL CONTRATO

C. EDUARDO OROPEZA ORTÍZ
Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional

BBN/CFRD /LBGP/VER

	INSTITUTO MEXICANO DEL SEGURO SOCIAL **DIRECCIÓN DE ADMINISTRACIÓN** **UNIDAD DE ADQUISICIONES E INFRAESTRUCTURA** **COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS** **COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS**	**Contrato Número** **P0M0026**

ANEXO 1

"DICTAMEN DE DISPONIBILIDAD PRESUPUESTAL PREVIO, ANEXO TÉCNICO Y TÉRMINOS Y CONDICIONES"

ANEXOS

DIVISIÓN DE CONTRATOS

EL PRESENTE ANEXO CONSTA DE **144** HOJAS INCLUYENDO ESTA CARÁTULA

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

SIN TEXTO

0183

INSTITUTO MEXICANO DEL SEGURO SOCIAL

DIRECCION DE FINANZAS
UNIDAD DE OPERACIÓN FINANCIERA
COORDINACIÓN DE PRESUPUESTO E INFORMACIÓN PROGRAMÁTICA
DICTAMEN DE DISPONIBILIDAD PRESUPUESTAL PREVIO

FOLIO: 0000002003-2020

☐ Dictamen de Inversión
☒ Dictamen de Gasto

Dependencia Solicitante: 09 Distrito Federal Nivel Central
099001 Oficinas Centrales
580000 Coord de Servicl Administra

Concepto: OFICIO No. 1788 RECIBIDO EL 30OCT2019 CONTRATACIÓN DE LOS "SERVICIOS DE CONTINUIDAD DE LA NUBE IMSS 2020"

Fecha Elaboración: 30/10/2019

Importe Comprometido (en pesos): $ 750,000,000.00
Cuenta: 42061506 SERV. INT. TEC DE INFO. Y COM. Unidad de Información: 099001 Centro de Costos: 500000

COMPROMETIDO MENSUAL (en miles de pesos):

ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
750,000.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

DISPONIBLE (en miles de pesos):

1,504,775.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

El presente documento de existencia de respaldo presupuestario se emite en términos de lo señalado en numeral 7.2.10 de la Norma Presupuestaria del Instituto Mexicano del Seguro Social (IMSS), y de lo establecido en el artículo 8°, 144 y 148 del Reglamento Interior del IMSS. responsabilidad del área solicitante el destino y aplicación de los recursos. También se informa que este documento únicamente tendrá validez para el ejercicio fiscal en curso, y que con base en la revisión que se efectuó en el Sistema Financiero PREI-Millenium, en el Módulo de Control de Compromisos, en la combinación unidad de información y centro de costos, los montos señalados quedan comprometidos para dar inicio a las gestiones de adquisición de bienes y servicios con base al marco normativo vigente.

ATENTAMENTE

Lic. Jessica Miranda Vega
Titular de la División de Control y Seguimiento al Gasto de Operación

DIA	MES	AÑO

DICTAMINADO DEFINITIVO

DICTAMEN DEFINITIVO

CONTRATO No. _____

_____

IMPORTE DEFINITIVO (EN PESOS) : $ _____ .00

SE EMITE SUJETO A LAS CIFRAS DEFINITIVAS QUE APRUEBE LA H. CÁMARA DE DIPUTADOS PARA EL IMSS, RAZÓN POR LA CUAL EL IMPORTE DEBERÁ RATIFICARSE UNA VEZ QUE SE TENGA EL PRESUPUESTO APROBADO PARA EL EJERCICIO 2020.

Clave: 6170-009-001

INSTITUTO MEXICANO DEL SEGURO SOCIAL
COORDINACIÓN TÉCNICA DE GESTIÓN PRESUPUESTARIA
DIVISIÓN DE CONTROL Y SEGUIMIENTO AL GASTO DE OPERACIÓN
CERTIFICADO PRESUPUESTAL

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

Anexo Técnico

Servicio de Continuidad de la Nube IMSS 2020

2020

ANEXOS
DIVISIÓN DE CONTRATOS

Contenido

ANEXOS

DIVISIÓN DE CONTRATOS

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	14/10/2019	Elaboración de documento	Ing. Héctor Javier Reyes Oropeza Lic. Carlos Francisco Ramírez del Rivero Ing. Héctor Martínez Valenzuela Ing. Alejandro Paniagua Ramírez
0.2	28/10/2019	Actualización del documento	Ing. Javier Cortés López Ing. Carlos Calderón Zacarías
1.0	12/11/2019	Aprobación del documento	Ing. Eduardo Oropeza Ortiz

1. OBJETIVO DEL DOCUMENTO

Elaborar el Anexo Técnico que contenga los requerimientos y las especificaciones técnicas del bien o servicio de TIC que se pretenda contratar.

Clasificador Único de las Contrataciones Públicas (CUCOP): 31900002

2. OBJETIVO

Brindar continuidad operativa de los servicios que permiten al Instituto disponer de las capacidades de procesamiento, almacenamiento, respaldo, comunicaciones, seguridad, plataformas tecnológicas y software bajo las **modalidades de despliegue** siguientes:

- **M1**: Centro de Datos externo (Centro de Datos Primario),
- **M3**: Extensión de Nube Privada (ENP) en los puntos con mayor demanda transaccional de operación de los servicios del Instituto,
- **M5**: Instalaciones designadas por el Instituto, y
- **M6**: Ambientes no productivos para el apoyo a la evolución y desarrollo tecnológico

Estos servicios serán consumidos en tres modalidades:

- Los servicios relacionados a lo que se define como "**Nube Privada**", soportan entre otros, sistemas transaccionales del Instituto, aplicativos y tecnologías para servicios digitales y de información, bases de datos, medios de almacenamiento, software de productividad, y en general, aquellas tecnologías que están definidas expresamente para utilización del personal o para otorgar al público un servicio del IMSS bajo control del mismo. Estos servicios deberán extenderse en las modalidades de despliegue de: Centro de Datos externo (Primario) y en Nodos de Extensión de la Nube Privada que se desplegarán conforme a lo indicado de manera referencial en el apéndice "Ubicaciones Geográficas".

- Los servicios relacionados a lo que se define como "**Nube Híbrida**", soportan los servicios aplicativos, digitales y de información, que requieren la interconexión con nubes públicas, privadas y comunitarias. Estos servicios contarán con la capacidad de intercambio de tráfico entre redes de telecomunicaciones, despliegue de canales digitales con reglas específicas de comunicaciones y seguridad, así como la capacidad de extensión de la nube híbrida en regiones geográficas estratégicas para mejorar la experiencia a usuarios externos en la entrega de servicios.

- Los servicios que se definen como de "**Integración a la Nube Privada**", se refieren a la capacidad de consumo tecnológico en las instalaciones designadas por el Instituto, con la finalidad de lograr algún nivel de integración, desde la capacidad de ser accedida a nivel telecomunicaciones, hasta poder consumir o entregar información desde o hacia la Nube Privada.

Los diferentes servicios incluidos dentro de los servicios dentro del presente Anexo Técnico, serán diferenciados tanto por la modalidad de despliegue como la modalidad de Nube. La modalidad de despliegue de Ambientes no productivo, aplicará a las tres modalidades de nube: Privada, Híbrida y de Integración a la Nube Privada.

Los servicios serán medidos a través de acuerdos de Niveles de Servicio, para buscar un uso eficiente y eficaz de los servicios y soluciones, apego a procesos determinados por la normatividad del Instituto, así como el suministro de hardware y software para soporte de las aplicaciones del Instituto, lo que permitirá:

- Flexibilizar y agilizar la atención gradual de requerimientos de infraestructura tanto física como virtual.
- Mantener niveles de operación y de seguridad para la Institución.
- Continuidad en la operación de los servicios digitales y de información, así como de los sistemas informáticos del Instituto.
- Contar con alojamiento de las capacidades de infraestructura y almacenamiento.
- Establecer una estrategia en materia tecnológica para el procesamiento y almacenamiento de información del Instituto, así como el de las plataformas que soportan servicios digitales y de información.
- Monitorear el desempeño de los recursos, dar visibilidad de la disponibilidad de servicios digitales y de información, así como la ejecución de actividades de aprovisionamiento y mantenimiento de infraestructura y plataformas con base en Acuerdos de Nivel de Servicio (SLA's).
- Mantener un esquema de atención a derechohabientes, patrones, proveedores, terceros relacionados y/o público en general que ocupe las diversas aplicaciones, servicios digitales y de información que el Instituto ofrece a través de los diversos canales de atención del Instituto, incluyendo portal de Internet (www.imss.gob.mx), conexiones con terceros, ventanilla, notificaciones y canal móvil, así como contribuir a la transformación digital del Instituto y la atención que presta a sus derechohabientes y patrones.

Resumen de la situación actual

Durante el periodo del 2016 al 2019, el Instituto ha contado con un centro de datos primario, administrado por un tercero. En ese mismo período, el Instituto ha brindado continuidad de los servicios del Instituto y desplegado plataformas tecnológicas para la generación de servicios digitales a través de múltiples canales de atención.

El servicio actual de centro de datos tercerizado ha permitido la operación de diversos sistemas sustantivos del Instituto, dando cobertura a la operación institucional de al menos:

- 84 millones de asegurados y derechohabientes,
- Aproximadamente 1 millón de patrones,
- Aproximadamente 3 millones de pensionados.
- Aproximadamente 460,000 empleados IMSS.
- Aproximadamente 3,000 inmuebles IMSS.

A través de la operación de los servicios tecnológicos en el actual centro de datos tercerizado, el Instituto ha atendido desde agosto de 2013 a junio del 2019, los siguientes trámites:

- 656.4 millones de trámites digitales.
- Recaudación de aproximadamente $1,400 millones de pesos diarios.
- Movimientos Afiliatorios de 986 mil patrones.
- 51 millones de pagos referenciados.
- 11 millones de citas médicas desde la app móvil.
- 9.1 millones de expedientes electrónicos.
- 14.4 millones de recetas electrónicas expedidas.

- 18.5 millones de constancias de semanas cotizadas.
- 128.1 millones de avisos para control de servicios integrales.
- 8.4 millones de cuentas por pagar.
- De 5 a 7 millones de consultas de vigencia de derechos diarias,
- Operación de aproximadamente 160 sistemas, aplicativos y servicios en el centro de datos administrado principalmente de temas de Afiliación, Incorporación, Recaudación, Cobranza, Pensionados, Prestaciones Médicas, Financieros, Administrativos y Jurídicos, entre otros.

Los servicios del centro de datos tercerizado también apoyan temas médicos, dentro de los que destacan los siguientes servicios **diarios**.

- 504 mil 776 consultas.
- 54 mil 958 urgencias.
- 3 mil 861 intervenciones quirúrgicas.
- Mil 36 partos.
- 353 mil 634 consultas de especialidad.

El centro de datos tercerizado también apoya en temas de recaudación, de tal manera que el Instituto recauda aproximadamente 1,400 millones de pesos diarios.

Finalmente este tipo de servicios reflejan la necesidad de brindar la continuidad en la operación y gestión de la operación 7X24X365 a fin de garantizar los servicios que el Instituto ofrece a los derechohabientes, patrones, contribuyentes, pensionados, personal institucional y público en general.

En el **Apéndice "Relación de Infraestructura actual en Centro de Datos y proyección de crecimiento"** se describe la relación de la infraestructura que abarcan dichos sistemas legados y plataformas, misma que deberá ser considerada como la línea base de estimación de costos a partir de la migración y puesta en producción de los servicios de descritos en el presente anexo técnico.

Para lo anterior, se requiere que el **LICITANTE** ofrezca el servicio de habilitación de infraestructura tecnológica, migración de dicha infraestructura, servicios digitales y aplicaciones a su centro de datos a fin de garantizar la continuidad operativa de los servicios del Instituto que actualmente se encuentran alojados en el Centro de Datos tercerizado.

ANEXOS

DIVISIÓN DE CONTRATOS

3. ALCANCE

El **LICITANTE** deberá incluir en su propuesta realizar las actividades necesarias para brindar continuidad operativa a los servicios del presente anexo técnico, para el aprovisionamiento de infraestructura de procesamiento, almacenamiento, respaldos, comunicaciones, licenciamiento, seguridad informática perimetral y en su caso actividades de migración de centro de datos para que el Instituto opere tal y como se describe en el apéndice "Relación actual de Infraestructura en Centro de Datos y proyección de crecimiento", durante el periodo del 1 de enero al 31 de diciembre de 2020, incluyendo el proceso de migración necesario de centro de datos conforme al Plan General de Trabajo ofertado por el **LICITANTE**, tomando las medidas necesarias para garantizar la continuidad del servicio actual.

El **LICITANTE** deberá ofertar en su propuesta económica el costo del concepto de migración bajo el rubro "migración de centros de datos", incluyendo los tiempos de posible afectación a la operación debido a los procesos de migración de información, aplicativos, sistemas y servicios electrónicos o digitales del IMSS del Centro de Datos Actual a la infraestructura ofertada por el **LICITANTE**, tanto al interior del Instituto como con los Organismos con los que éste interopera, tales como Servicio de Administración Tributaria (SAT), Registro Nacional de Población (RENAPO), Comisión Nacional Para el Sistema de Ahorro para el Retiro (CONSAR), Infonavit, ProceSar, Afores, Bancos, Instituto Nacional Electoral (INE), entre otros, con los cuales el IMSS intercambia información e interopera procesos de negocio en su gran mayoría en línea o mediante procesos de bloques sincronizados, incluyendo los procesos de sincronización que se realizan diariamente entre los principales sistemas y servicios operados en el centro de datos administrado y el ecosistema IBM Mainframe ubicado en los centros de datos Institucionales, en los que se sincroniza diariamente la información de recaudación, vigencia de derechos, movimientos Afiliatorios y en general toda la sincronización entre los principales sistemas y aplicativos institucionales.

Adicionalmente, el **LICITANTE** deberá incluir en su propuesta la habilitación de infraestructura, así como mantener la continuidad operativa de la solución de conectividad en red denominada "Punto Neutro", la cual concentra los enlaces de telecomunicaciones de las diferentes redes de telecomunicaciones del IMSS y proporcionadas por diversos LICITANTEes de servicio, así como los enlaces de telecomunicaciones de los principales organismos públicos y privados con los que el Instituto interactúa. Esto es, proporcionar la conectividad en red para los aproximadamente 3,000 inmuebles del IMSS donde interoperan con los sistemas y aplicativos ubicados en los Centros de datos centralizados, de igual manera realizan las consultas e interacciones con organismos terceros.

Así mismo, el Licitante deberá incluir en su propuesta la habilitación de infraestructura, así como la continuidad del servicio del centro de datos móvil ubicado en el Centro Médico Nacional de Occidente, en Guadalajara Jalisco, el cual contempla los servicios virtualizados de cada uno de los aproximadamente 3,300 usuarios a través de aproximadamente 1,300 dispositivos clientes ligeros, así como todo el procesamiento y almacenamiento y sistemas de virtualización de cómputo que se requieren para soportar la solución citada.

Finalmente el Licitante deberá incluir en su propuesta que se requiere la habilitación de infraestructura, así como la continuidad del servicio de los aproximadamente 660 servidores de cómputo denominados "autocontenidos" los cuales se encuentran distribuidos a nivel nacional y que permiten la operación local de los Sistemas Integrales de Medicina Familiar (SIMF), SAI Farmacia, así como sistemas propios de cada

Unidad Médica, los cuales interactúan con los sistemas de cómputo centralizados que operan en el Centro de Datos Administrado.

El Licitante deberá ofertar en su propuesta la habilitación, instalación configuración, puesta a punto, interconexión de infraestructura, así como la migración de cada uno de los sistemas, aplicativos y servicio electrónicos que de forma enunciativa mas no limitativa, se enlistan en el apéndice 3, cuya operación debe garantizar la continuidad de los servicios que el Instituto presta a derechohabientes, patrones, pensionados, trabajadores del Instituto y público en general, a fin de interoperar dentro del ecosistema de infraestructura tecnológica del Centro de Datos administrado así como con los Centros de Datos Institucionales ubicados en Monterrey, Cd. De México y Guadalajara, además de los ecosistemas de infraestructura tecnológica con los que el IMSS interopera tales como: SAT, RENAPO, Procesar, INFONAVIT, Bancos, Instituto Nacional Electoral, Afores, CONSAR, entre otros.

El **LICITANTE** deberá realizar las actividades correspondientes para soportar y operar la infraestructura, aplicaciones y servicios en cualquiera de las modalidades descritas en el presente anexo técnico, garantizando los niveles de servicio señalados en el apartado "Niveles de Servicio" a fin de brindar continuidad a los procesos de negocio internos y externos al IMSS.

El alcance de los servicios descritos en este Anexo Técnico comprende los siguientes elementos, conforme a los servicios descritos más adelante:

- Continuidad operativa y aprovisionamiento bajo demanda de los Bloques de Construcción Fundamentales (BCF) conforme se especifica en el Apéndice "Bloques de Construcción Fundamentales" correspondiente, de acuerdo a cada solicitud específica del Instituto.
- Aprovisionamiento bajo demanda de los Bloques de Construcción Comunes (BCC), partiendo de un ejercicio de planeación con el Instituto para determinar las diferentes plataformas que se requieren; y con base en ellas, establecer la definición y habilitación de los BCC a partir de los BCF.
- Monitoreo y vigilancia del funcionamiento y desempeño de los BCF y BCC, así como de los servicios digitales y de información, y los sistemas informáticos y canales digitales que los soportan y se determinen por el Instituto.
- Continuidad Operativa de la interconexión entre múltiples redes privadas de telecomunicaciones a través de un Punto Neutro de intercambio de tráfico, así como el despliegue de canales de acceso con otras nubes tanto públicas como privadas, en la que destaca el acceso a Internet y varias dependencias públicas, mismas que se identifican en el apéndice "Relación actual de la Infraestructura en Centro de Datos".
- Continuidad Operativa y en su caso aprovisionamiento e instalación de cada nodo de extensión de la nube privada, configuración, puesta en marcha, operación, mantenimiento, soporte y administración de Puntos de Acceso a la Nube Privada con capacidad de despliegue del servicio de Escritorio en la nube.
- Provisión de servicios de administración y monitoreo relacionados a los BCF y BCC de la solución.
- Seguridad y autocontenidos

Una vez iniciados los servicios, el LICITANTE deberá brindar continuidad operativa a los servicios del presente anexo técnico y dar cumplimiento al Plan de Trabajo Detallado ofertado, al amparo y cumplimiento del Plan de Trabajo General descrito en este documento, con el cual en cuyo caso efectuará la migración de elementos dispuestos en el Servicio actual de Centro de Datos. Una vez que los BCF correspondientes a la

ANEXOS
DIVISIÓN DE CONTRATOS

migración se encuentren activos y operando en el Centro de Datos ofertado a entera satisfacción del Instituto, podrán ser incorporados al esquema de contraprestación de pagos mensuales.

En apego al mismo Plan de Trabajo General, el licitante deberá presentar en su propuesta un programa de trabajo anual para cada uno de los siguientes servicios:

- Servicio de Continuidad y Gestión de la Operación
- Servicio de Operación y Calidad de la Seguridad informática perimetral
- Servicio de integralidad de ambientes distribuidos a nivel nacional y telecomunicaciones
- Servicio de Gestión de Medición del Desempeño de Aplicativos y Componentes Institucionales

Una vez ofertados y detallados por el licitante estos planes de trabajo en su oferta, y en su caso revisados, modificados, detallados y finalmente aceptados por el Instituto en las reuniones de inicio del contrato, el licitante deberá comenzar a realizar las actividades de habilitación, implementación, puesta punto, operación y administración de cada servicio.

El plan de trabajo general propuesto por el **LICITANTE** podrá sufrir modificaciones durante su ejecución de acuerdo a las necesidades operativas del Instituto, por ejemplo, en casos donde resulte inviable migrar aplicativos o servicios por la alta concurrencia, alta demanda o estacionalidad de negocio en un periodo especifico, por lo que habrá que esperar las condiciones operativas necesarias que permitan ejecutar la migración, tal es el caso de los periodos de alta recaudación, emisión, dictaminación, cierres presupuestales, por mencionar algunos.

Vigencia

La vigencia del contrato y el plazo para la para la prestación del servicio será a partir del día hábil siguiente del acto de notificación de fallo y hasta el 31 de diciembre de 2020.

Modalidad del Servicio

El modelo de servicio en el presente Anexo Técnico, toma como base el concepto de "servicios administrados bajo demanda", que involucra un precio unitario por unidad devengada en un periodo determinado, así como pago de servicios relacionados a la operación, seguridad, telecomunicaciones y migración, que brinden la continuidad de la operación a los servicios institucionales que se encuentran alojados en el centro de datos del **LICITANTE** acorde a los niveles de servicio establecidos. El modelo del servicio incluye las siguientes características o funcionalidad:

El licitante deberá incluir en su oferta: habilitar, migrar, implementar, configurar, poner a punto, operar y administrar el servicio de Continuidad Operativa de los sistemas actuales de procesamiento y almacenamiento con la siguiente funcionalidad y características:

- Aprovisionamiento de hardware y software bajo una modalidad de servicios administrados bajo demanda.

- Capacidad de soportar operativamente soluciones de TIC complejas a través de la correcta implementación de Bloques de Construcción Comunes (BCC), basados en niveles de servicio y características de los Bloques de Construcción Fundamentales (BCF). Los bloques de construcción fundamentales son las pieza mínimas indivisibles para efecto de facturación y cobranza del presente servicio, mientras que los bloques de construcción comunes son conjuntos de BCF que se agrupan para la habilitación de una solución de negocio, tales como el Expediente Clínico Electrónico o cualquier otro sistema integral operativo, por lo que estos nuevos bloques (BCC) serán considerados para la cuantificación de la deductiva de la infraestructura en caso de falla de un servicio de negocio con afectación a infraestructuras dependientes o correlacionadas con la misma, las cuales dejan de operar por consecuencia de la falla de una infraestructura diferente, lo que ocasionará que las deductivas aplicables incluyan tanto a los BCF afectados, como a los BCC correlacionados que sufren afectación a causa de terceros.
- Monitoreo de la infraestructura y la visibilidad sobre la situación operativa de la infraestructura y de los diferentes servicios tecnológicos, digitales y de información que el Instituto señale.
- Servicios de Soporte a la Operación apegados a las "buenas prácticas" nacionales e internacionales y en general la normatividad aplicable durante la prestación del servicio.
- Servicios operativos de seguridad de la información a través de un Centro de Operaciones de Seguridad (SOC).
- Identificación de actividades para garantizar la escalabilidad, prever disminución y aumentos en la demanda de recursos tecnológicos en función del análisis periódico de crecimiento y uso de recursos.
- Proponer mejoras a la forma de disposición de los BCF y los BCC para generar eficiencias y mejora en el desempeño.
- Gestión continua de problemas conocidos y análisis de los mismos para identificar causas raíz y propuesta de mejora.

El licitante deberá incluir como parte del servicio: habilitar, migrar, implementar, configurar, poner a punto, operar y administrar toda la infraestructura necesaria para efectuar las acciones para el abatimiento del rezago tecnológico en infraestructura, sistemas y tecnologías o actualización tecnológica, por medio de:

- En general, todas las acciones de remediación que el licitante o el Instituto proponga a fin de restaurar los niveles de servicio en caso de falla continua (intermitencias en la operación al menos tres veces en un mismo mes) que se traduzca en una afectación a los niveles de servicio y operación institucional.
- Actualizaciones tecnológicas que correspondan, que deberán traducirse en ajustes, sustituciones, reemplazos, compensaciones, escalamientos, adaptaciones y demás acciones análogas que reflejen la forma en que el prestador del servicio entrega al Instituto cada uno de los servicios que se comprenden en este Anexo Técnico.
- Actividades continúas de mantenimiento tecnológico a fin de mejorar la experiencia de servicio entregado al Instituto, así como mejorar los niveles de servicio y aceptación de los usuarios institucionales.

Mínimos y Máximos

El esquema de consumo de los servicios del presente anexo técnico será basado en mínimos y máximos, los cuales serán devengados en una primera etapa por los servicios de migración de centro de datos, por el consumo de BCF conforme a la "Relación de inventario actual de Centro de Datos"; de manera similar se consumirán los servicios de Centro de Operaciones de Seguridad y del Centro de Continuidad Operativa que serán considerados a partir de la toma en administración de los servicios. A partir de dicho momento, se consumirán los BCF y los BCC sobre demanda, tal y como se establece a lo largo del presente documento.

a) Arquitectura de referencia del presente anexo técnico

En el marco de la Transformación Digital IMSS, se establece una estrategia basada en un modelo de 'nube', que busca fomentar la reutilización, recursos compartidos, y agilidad en el despliegue de soluciones y servicios, previendo la capacidad para acceder de manera flexible a un diverso número de recursos informáticos virtuales asignados de forma ágil y dinámica, obteniendo así la capacidad de procesamiento, almacenamiento, respaldos, seguridad y comunicaciones necesarios.

En las siguientes subsecciones se presenta un marco teórico de referencia sobre el concepto de nube, en ningún momento se deberán considerar como requerimientos puntuales si no son señalados explícitamente en alguna otra sección del presente Anexo Técnico.

a.1. Capacidades del cómputo en la nube

Según los mismos estándares citados anteriormente, para poder describir eficazmente cuáles son las claves del concepto del Cómputo en la Nube, se recurre a una serie de capacidades o características principales que lo diferencian de los sistemas tradicionales de explotación de las TIC. Entre las capacidades asociadas al Cómputo en la Nube se encuentran las siguientes:

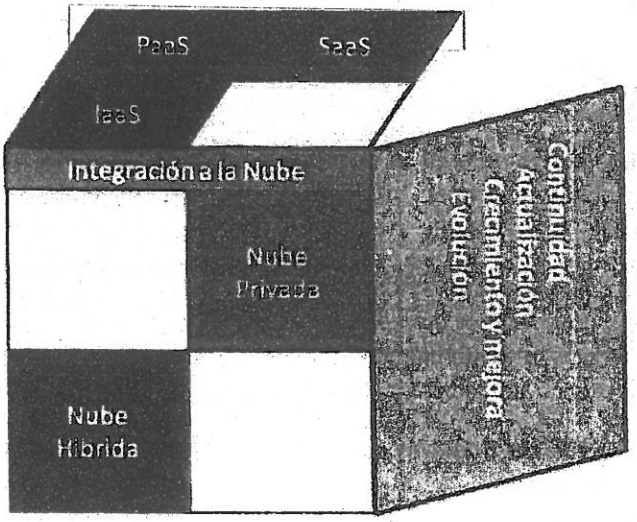
1. **Facturación basada en el consumo**. - Una de las características principales de las soluciones de nube es el modelo de facturación basado en el consumo, es decir, el pago varía en función del consumo que se realiza del servicio en la nube contratado, por lo que el pago es sobre servicios debidamente devengados.
2. **Abstracción**. - Característica o capacidad de aislar los recursos informáticos contratados al LICITANTE de servicios en la nube de los equipos informáticos del cliente. Esto se consigue gracias a la virtualización, con lo que la organización usuaria no requiere de personal dedicado al mantenimiento de la infraestructura, actualización de sistemas, pruebas y demás tareas asociadas que quedan del lado del servicio contratado, al mismo tiempo, que se mantiene un orden y gobierno para evitar el caos en el consumo de virtualización.
3. **Agilidad en la escalabilidad (elasticidad)**. - Capacidad que permite aumentar o disminuir las funcionalidades ofrecidas al cliente, en función de sus necesidades puntuales. Esta característica, relacionada con la de Facturación basada en el consumo, evita los riesgos inherentes de un posible mal dimensionamiento inicial en el consumo o en la necesidad de recursos,
4. **Multi-Consumidor**. - Capacidad que otorga la nube para permitir que varios consumidores (aplicaciones, usuarios, áreas del Instituto o inclusive terceros como instituciones) compartan los medios y recursos informáticos, permitiendo la optimización de su uso.
5. **Autoservicio bajo demanda**. - Esta capacidad permite al consumidor acceder de manera flexible a las capacidades de computación en la nube de forma automática a medida que las vaya requiriendo, sin necesidad de una interacción humana con su **proveedor** o **proveedores** de servicios en la nube.
6. **Acceso sin restricciones**. - Capacidad consistente en la posibilidad ofrecida a los consumidores de acceder a los servicios consumidos de la nube en cualquier lugar, en cualquier momento y con cualquier dispositivo que disponga de conexión a redes de protocolo TCP/IP o a la red privada del Instituto en el caso de la Nube Privada. El acceso a los servicios de la nube se realiza a través de la red, lo que facilita que distintos dispositivos, tales como teléfonos móviles, dispositivos PDA u ordenadores portátiles, puedan acceder a un mismo servicio ofrecido en la red mediante mecanismos de acceso comunes.

El **LICITANTE** deberá a través de los servicios del presente anexo técnico cubrir las capacidades de cómputo en la nube antes mencionadas o las necesarias para su operación.

a.2. Características del cómputo en la Nube

Las soluciones de cómputo en la nube disponibles en el mercado en la actualidad admiten diferentes clasificaciones según el aspecto que se tenga en cuenta para realizar dicha clasificación. Con base en las definiciones de industria consideradas en los estándares del Instituto dentro del marco de la Transformación Digital IMSS, se definen tres características fundamentales que marcan la definición de modelos para las soluciones de nube: familias, formas de implementación y capacidades técnicas del LICITANTE.

Mediante la combinación de estas tres dimensiones se detallan los distintos modelos de cómputo en la nube existentes en el mercado. Estas tres características, junto con sus diferentes tipos de soluciones asociadas, se pueden representar en un cubo de tres dimensiones. La selección de las características que aplican a los servicios del presente Anexo Técnico, se muestran bajo el modelo de cubo en la imagen siguiente:



Representación gráfica de características y tipos de soluciones de nube seleccionadas

Clasificación por familias de tecnologías como servicio

Infraestructura como un servicio (IaaS)

Familia del Cómputo en la Nube consistente en poner a disposición del cliente el uso de la infraestructura informática (capacidad de computación, espacio de disco y bases de datos, entre otros) como un servicio.

Los clientes que optan por este tipo de familia de nube, en vez de adquirir o dotarse directamente de recursos como pueden ser los servidores, el espacio del centro de datos o los equipos de red, optan por la

tercerización o provisión de infraestructura mediante servicios proporcionados por un tercero (externalización en busca de un ahorro en la inversión en sistemas de TI).

Con esta externalización, las facturas asociadas a este tipo de servicios se calculan con base en la cantidad de recursos consumidos por el cliente, basándose así en el modelo de pago por uso.

Plataforma como un Servicio (PaaS)

Familia del Cómputo en la Nube, consistente en la entrega como un servicio, de un conjunto de plataformas informáticas orientadas al desarrollo, pruebas, despliegue, alojamiento y mantenimiento de los sistemas operativos y aplicaciones propias del cliente.

Las principales características asociadas a la Plataforma como Servicio, como solución de nube, se exponen a continuación:

1. Facilita el despliegue de las aplicaciones del cliente, sin el costo y la complejidad derivados de la compra y gestión del hardware y de las capas de software asociadas.
2. Ofrece, a través de redes de servicio IP, todos los requisitos necesarios para crear y entregar servicios y aplicaciones web.

Software como un Servicio (SaaS)

Familia del Cómputo en la Nube consistente en la entrega de aplicaciones como servicio, siendo un modelo de despliegue de software mediante el cual el **LICITANTE** ofrece licencias de su aplicación a los clientes para su uso como un servicio bajo demanda.

Los Proveedores del Software como Servicio pueden tener instalada la aplicación en sus propios servidores Web (permitiendo a los clientes acceder, por ejemplo, mediante un navegador web), o descargar el software en los sistemas del servicio de nube. En este último caso, se produciría la desactivación de la aplicación una vez finalice el servicio o expire el contrato de licencia de uso.

La solución de cómputo en la nube de Software como Servicio puede estar orientada a distintos tipos de clientes según su condición, por ejemplo:

- Servicios de productividad en la nube.
- Correo electrónico.
- Escritorio en la nube.
- Colaboración.

a.3. Bloques de construcción

Para fines del presente Anexo Técnico un bloque de construcción (BB, Building Block por sus siglas en inglés) se entiende como un componente unitario o aislado del modelo completo de la arquitectura que describe el modelo completo. Representa un paquete de funcionalidad definido para satisfacer una o varias de las necesidades del Instituto. Los bloques de construcción son tipificados como: una función o capacidad técnica, un componente de aplicación o un componente tecnológico, por citar algunos ejemplos; los cuales pueden interoperar con otros bloques de construcción, componerse de, o ser parte de, otros bloques de construcción.

Los bloques de construcción representan los elementos categorizados dentro de la taxonomía del Instituto a través del continuo empresarial.

Bloques de Construcción Fundamentales (BCF)

Los BCF se definen como aquellos Bloques de Construcción que se encuentran descritos en el Apéndice "Bloques de Construcción Fundamentales".

Bloques de Construcción Comunes (BCC)

Los BCC son aquellos Bloques de Construcción que se definen a partir de múltiples BCF, con la finalidad de crear elementos de mayor funcionalidad y complejidad los servicios del presente anexo técnico, pero con cierto grado de generalidad que hacen factible su reutilización para múltiples soluciones. Los BCC serán definidos de manera conjunta entre el LICITANTE y el Instituto durante la vigencia del servicio.

a.4. Estrategia de disponibilidad y niveles de servicio

Los servicios objeto del presente Anexo Técnico consideran los elementos y las acciones necesarias para que dichos servicios se encuentren operando y sean accesibles conforme a los niveles de servicio que requiere el Instituto; para lo cual se alinearán a lo señalado en el MAAGTICSI y las "buenas prácticas" que señala la industria (en particular ITIL), en cada uno de sus componentes y procesos del ciclo de vida de entrega del servicio.

El **LICITANTE** cumplirá con los niveles de servicio establecidos en el presente Anexo Técnico o en el apéndice respectivo, soportado en la capacidad actual de la infraestructura en operación, y en las proyecciones para los nuevos servicios incluidos en el portafolio de servicios del Instituto, incluyendo los siguientes rubros:

- Información relevante que se desprenda en las capacidades de la infraestructura.
- Requerimientos, actuales y previstos, de disponibilidad de los servicios objeto del presente Anexo Técnico.
- Disponibilidad de los componentes de la infraestructura de TIC que soportan los servicios del contrato, incluidos los relacionados que sean proporcionados por terceros.
- Riesgos que pudieran materializarse al efectuar adecuaciones a los componentes de la infraestructura que soportan los servicios.
- Costos estimados y validados por el Instituto para llevar a cabo las adecuaciones que permitan obtener la disponibilidad esperada acorde a los niveles de servicio.
- Reporte mensual de la disponibilidad de los servicios para determinar el cumplimiento de los niveles de servicio descritos en el presente anexo técnico, en función de la disponibilidad de la infraestructura y componentes asociados que soportan los servicios.
- Reporte de los incidentes que se han presentado por falta de disponibilidad identificados a través las herramientas de visibilidad del servicio y gestionadas mediante el Servicio de Continuidad Operativa.
- Evaluación de los niveles de disponibilidad de los servicios y de los componentes de la infraestructura que los componentes con respecto a:
  - Los niveles de servicio originalmente acordados.
  - Los niveles de servicio efectivamente proporcionados.
  - Los niveles de servicio que, de acuerdo con el programa de disponibilidad.
- Configuración en una base de datos de gestión de configuraciones (CMDB) y las características de cada componente de la infraestructura que soportan los servicios.

- Mecanismos de comunicación hacia los responsables de los dominios tecnológicos involucrados en los servicios objeto del presente Anexo Técnico para que estén informados de:
  - Las oportunidades identificadas para mejorar la disponibilidad de los servicios.
  - Recomendaciones sobre los incidentes por falta de disponibilidad.
- Niveles de servicio alcanzados.

a.5. Planeación y gobierno

La DIDT ha implementado, como parte de su modelo gobierno, un conjunto de acciones que le permiten enfocar sus iniciativas hacia la habilitación y continuidad de la Estrategia del Instituto, de tal manera que dicha oferta se encuentre alineada con los objetivos y necesidades de negocio del Instituto a nivel estratégico, a través del establecimiento de la demanda de servicios desde un ejercicio de planeación.

Como parte de los procesos de planeación y gobierno de la DIDT establecidos en su modelo de operación, se encuentran estrechamente relacionados los procesos de Planeación Estratégica, pues es a través de estos procesos que se genera el portafolio estratégico de proyectos (PEP) definido por la DIDT.

Los Servicios del presente Anexo Técnico, deberán estar alineados al PEP y de ser necesario, si el Instituto así lo señala, participar en mesas de trabajo para aportar en la definición de dicho instrumento, brindando información respecto de la operación, capacidades y situación actual de los servicios del presente Anexo Técnico.

Planeación y gobierno

El **LICITANTE** participará en el establecimiento de la hoja de ruta de arquitectura Institucional, así como en el desarrollo la planeación de la implementación para los trabajos de arquitectura conforme a los programas y proyectos establecidos por el Instituto. También debe integrarse para su operación con los marcos de trabajo vigentes en el Instituto para la gestión de proyectos, modelos de gobierno tecnológicos, modelos de gestión de contratos, etc.

Recomendación tecnológica

El LICITANTE deberá emitir recomendaciones y propuestas relacionadas a la continuidad de la operación de los servicios institucionales y de conformidad con el alcance de los servicios del presente anexo técnico.

Evolución tecnológica

El **LICITANTE** deberá como parte del servicio de continuidad de la operación y en caso de que aplique, presentar al Instituto las propuestas de acuerdo a los requerimientos y tendencias tecnológicas que se identifiquen durante la vida del contrato, que fomenten la continuidad de los servicios ofertados en el presente anexo técnico.

Gestión del conocimiento

El **LICITANTE** como parte de los servicios del presente anexo técnico, deberán consolidar la información y permitir al Instituto acceder a las bases del conocimiento relacionado con los servicios del presente anexo técnico, vigilando en todo momento el cumplimiento del marco jurídico en conjunto con el Instituto.

b) Plan de Trabajo General

El Plan de Trabajo General especifica las fases más relevantes del contrato, el **LICITANTE** deberá entregar el plan de trabajo y establecer los tiempos máximos que prevé emplear en cada una de ellas a fin de dar cumplimiento de las obligaciones relacionadas a los servicios del presente anexo técnico.

Servicio de Continuidad de la Nube 2020

Marco de referencia del Plan de Trabajo General

El **LICITANTE** en su propuesta deberá incluir el Plan de Trabajo General, que deberá especificar hitos y fases para el cumplimiento de los servicios del presente anexo técnico, mismos que serán respetados en todo momento tanto en fechas y compromisos establecidos como en el alcance y funcionalidad ofertada. El **LICITANTE** deberá de integrar en su propuesta, las definiciones o peticiones de servicio que se establecen en este Anexo Técnico y que son vinculadas a una o más fases del Plan de Trabajo General.

A continuación, se especifica de manera enunciativa más no limitativa, una tabla-resumen de los hitos que se prevén en el Plan de Trabajo General para los servicios descritos en el presente anexo técnico, indicando Fase, Identificador del hito en cuestión (ID), el nombre o descripción del hito, las fechas relativas y absolutas de inicio y/o término, cantidad de días naturales máximos de duración por hito que el posible **LICITANTE** oferte.

Tabla Hitos relevantes a considerar en el Plan de trabajo

Fase	ID	Hito	Inicio / Término máximo del Hito	Máxima duración en días naturales**	Prede nte(s)
Proceso de Migración de Centro de Datos actual al Servicio de Continuidad de Nube IMSS 2020.					
Planeación del Arranque	1	Kick-Off y presentación del equipo de trabajo del **LICITANTE.**	A más tardar 10 días naturales posteriores al Fallo	Plazo ofertado por el posible **LICITANTE**	N/A
	2	Mesas (sesiones) de trabajo de Planeación del Arranque, entre el **LICITANTE** y el IMSS, convocadas por el Grupo Administrador del Contrato IMSS	Plazo ofertado por el posible **LICITANTE**	Plazo ofertado por el posible **LICITANTE**	1
	3	Presentación, por parte del **LICITANTE** del Plan de Trabajo Detallado	A más tardar 5 días naturales posteriores a la finalización de las Mesas de Trabajo	Plazo ofertado por el posible **LICITANTE**	2
	4	Análisis y Revisión (en su caso aprobación) del Plan de Trabajo Detallado de parte del Grupo Administrador del Contrato del IMSS	A más tardar 15 días naturales posteriores a la entrega del Plan Detallado de parte del **LICITANTE**	Plazo ofertado por el posible **LICITANTE**	3
	5	En caso de aplicar, incluir firma de	A lo largo de los siguientes 25 días naturales a partir	Plazo ofertado por el posible	1

		Acuerdos de Nivel de Operación (OLAs) entre el **LICITANTE** y Terceros Involucrados en los servicios del presente anexo técnico.	del Kick-Off del proyecto	**LICITANTE**	
Actividades de migración de centro de datos actual y continuidad de la operación de servicios.	6	Inicio de actividades de migración del centro de datos actual al centro de datos del **LICITANTE** incluyendo servicios de punto neutro.	Al día natural siguiente a la aprobación, por parte del IMSS, del Plan de Trabajo Detallado	Plazo ofertado por el posible **LICITANTE**	4
	7	Finalización de actividades de migración del centro de datos actual al centro de datos del **LICITANTE** incluyendo punto neutro.	Plazo ofertado por el posible **LICITANTE**	Plazo ofertado por el posible **LICITANTE**	4
	8	Estabilización de los Niveles de Servicio a la finalización de la etapa de migración.	Plazo ofertado por el posible **LICITANTE**	Plazo ofertado por el posible **LICITANTE**	6 y 7
	9	Inicio de los Servicios asociados a la continuidad operativa de los servicios del presente anexo técnico.	Plazo ofertado por el posible **LICITANTE**	Plazo ofertado por el posible **LICITANTE**	N/A

ANEXOS
DIVISIÓN DE CONTRATOS

	10	Actividades de Finalización del Contrato.	A más tardar 4 meses naturales antes del día de la Finalización del Contrato	31 de diciembre de 2020	N/A
CIERRE	12	Finalización del Contrato	-	31 de diciembre de 2020	N/A

El **LICITANTE** deberá elaborar Programas de Trabajo Detallados que sean necesarios para la puesta a punto de cada uno de los servicios de:

- Servicio de Continuidad y Gestión de la Operación
- Servicio de Operación y Calidad de la Seguridad informática perimetral
- Servicio de integralidad de ambientes distribuidos a nivel nacional y telecomunicaciones
- Servicio de Gestión de Medición del Desempeño de Aplicativos y Componentes Institucionales

b.1. Consideración de la Migración de Punto Neutro

El servicio se dará por aceptado cuando se cumplan como mínimo los siguientes criterios:

- Cuando se logre la conexión en capa física y capa de 3 de la nube del **LICITANTE** de servicios ISP al Punto Neutro.
- En el caso del servicio de Internet y redes de MPLS, ejercer la conmutación en ambos "sites", (principal y secundario) para probar la redundancia geográfica.
- En un nodo o inmueble correr el protocolo de pruebas para todos los servicios y aplicaciones que la contratante determine, incluyendo si existe redundancia automática con algún otro proveedor ISP en la última milla.
- Cuando la herramienta de Monitoreo quede instalada en su totalidad para medir los SLA.
- Cuando queden firmados los SLA´s
- Cuando corra un mes de tiempo de garantía sobre los servicios.
- Cuando se entregue la memoria técnica de la solución.

En la entrega de documentación para procesos de Incidentes y cambios. Esquema propuesto para la prestación de los servicios solicitados deberá ser bajo la modalidad de servicios "Bajo Demanda", la cual se define de forma integral tanto en el anexo técnico como características técnicas de los servicios y en la propuesta económica por un precio unitario. Lo anterior permitirá la modalidad de poder realizar únicamente el pago por servicio devengado. Esta modalidad aplicará para los siguientes servicios:

- Servicios de aprovisionamiento de las soluciones de almacenamiento y recuperación de datos, procesamiento físico, infraestructura de red, y seguridad lógica.

- Servicio de piso blanco y de espacio en rack.
- Servicios de Monitoreo y Control de consumos de infraestructura.

4. CARACTERÍSTICAS DE LOS SERVICIOS

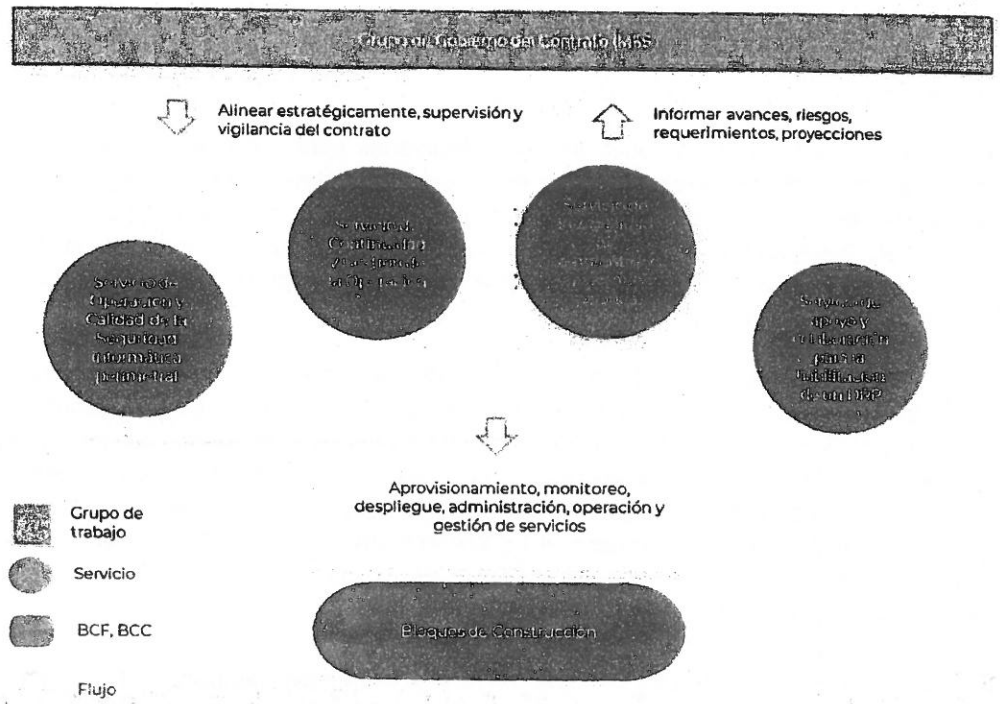
El servicio está compuesto por las siguientes categorías:

- Servicio de Continuidad y Gestión de la Operación
- Servicio de Operación y Calidad de la Seguridad informática perimetral
- Servicio de integralidad de ambientes distribuidos a nivel nacional y telecomunicaciones
- Servicio de Gestión de Medición del Desempeño de Aplicativos y Componentes Institucionales

El **LICITANTE** deberá asignar un responsable para dirigir la ejecución y el programa de trabajo de cada servicio, debiendo compartir actividades, recursos y responsabilidades entre los otros servicios del presente anexo técnico, buscando eficiencias y economías sin comprometer los niveles de servicio.

El objetivo primordial de los servicios del presente anexo técnico es de garantizar la continuidad operativa, gestión y el soporte de las plataformas, BCFs y BCCs realizando las actividades específicas necesarias para el sano funcionamiento del servicio.

La siguiente imagen muestra de manera esquemática el modelo operativo del servicio objeto del presente anexo técnico:



Marco Operativo base para el Servicio de Continuidad de la Nube IMSS 2020

4.1. Grupo de Gobierno del Contrato y aspectos generales para la prestación de los servicios del presente anexo técnico.

El Instituto informará al licitante los miembros del Grupo de Gobierno del Contrato (GGC), los cuales definirán, autorizarán y verificarán ante el **LICITANTE,** los requerimientos de servicios, así mismo recibirán la información de seguimiento de cada servicio, incluyendo el informe de avances, estado de requerimientos, asuntos, consumos, riesgos, desviaciones, incidentes, eventos, problemas, y cualquier información relacionada al servicio prestado.

El **LICITANTE** deberá de efectuar e informar al GGC del Instituto el seguimiento de cada servicio, informando avances, estado de requerimientos, asuntos, consumos, riesgos, desviaciones, incidentes, eventos, problemas, y cualquier información relacionada al servicio prestado.

El **LICITANTE** gestionará en conjunto con el GGC del Instituto toda la información generada por los servicios descritos en el presente anexo técnico y el licitante habilitará un repositorio de información donde deberá de integrar la información propia del contrato, entre otras, los entregables y documentación probatoria de la prestación de los servicios, a fin de que se cuente con la memoria documental de la operación y gestión de la operación en caso de que entes fiscalizadores soliciten la revisión de la documentación probatoria de la prestación de los servicios, esto no exime la entrega mensual en medios electrónicos y físicos de toda la información que se desprenda del presente anexo técnico.

El **LICITANTE** deberá apegarse al Marco Tecnológico de Referencia del Instituto en caso de ser necesario, buscando modelos de reutilización, estándares, modelos de referencia públicos relacionados al objeto del presente anexo técnico.

El **LICITANTE** deberá realizar las actividades técnicas necesarias para gestionar la información operativa relacionada a la ejecución de servicios descritos en el presente anexo técnico, identificando áreas de oportunidad y mejora operativa, mismas que serán informadas al GCC del Instituto para que en su caso sustenten la tomar decisiones en busca de la mejora en la continuidad operativa de los servicios del Instituto. Entregando al GCC la información relacionada a Incidentes, Problemas, Cambios, Eventos y la Base de datos de gestión de configuraciones (**CMDB**).

El **LICITANTE** con el objeto de contribuir al fortalecimiento de la supervisión y vigilancia de la administración del contrato materia del presente servicio y contribuir a las acciones para verificar la procedencia de los pagos, proporcionará al GCC todo el soporte documental acorde a lo establecido en los entregables del presente anexo técnico, indicando de manera formal las desviaciones respecto a los niveles de servicio acordados, así como la propuesta de cálculo de deductiva o penalización según sea el caso para cada servicio del presente anexo técnico. Del mismo el **LICITANTE** presentará al GCC la lista de obligaciones (entregables, verbos, entre otros) relacionadas al contrato y estrategia de atención, indicando en cuyo caso, las fechas límites para el cumplimiento de la obligación respetiva.

El **LICITANTE** con base en las solicitudes u órdenes de servicio que genere el Instituto en apego a lo descrito en el presente anexo técnico, presentara al GCC de manera semanal un desglose detallado del trámite que

corresponde a la atención de cada una de ella, en cuanto a su procedencia, tiempos límite de respuestas y demás circunstancias que se encuentren establecidas para cada servicio.

El **LICITANTE** proporcionará al GGC con base en la facturación mensual, la proyección del consumo de servicios hacia el final del contrato, que brinde información necesaria al Instituto para la toma de decisiones. Para lo anterior, el **LICITANTE** deberá entregar de manera semanal y mensual, el acumulado de BCF's facturados, con su correspondiente ejercicio presupuestal, proyección y tendencia de gasto durante la vigencia del contrato, así como su clasificación por centro de costo (por Dirección Normativa que consume los servicios) efectuando un prorrateo en caso de infraestructuras transversales.

4.2. Servicio de Continuidad a la Operación y Soporte

4.2.1. Soporte a la Continuidad Operativa

El **LICITANTE** deberá brindar continuidad operativa, gestión, operación y soporte a los Bloques de Construcción Fundamentales, Bloques de Construcción Comunes y los diversos componentes que integren los servicios tecnológicos que soportan las aplicaciones, componentes y servicios digitales del Instituto, a fin de dar cumplimiento a los niveles de servicio en el presente Anexo Técnico.

El **LICITANTE** deberá apegarse a las "buenas prácticas" en los procesos de gestión en materia de TIC, apegadas a la normatividad y los modelos de operación vigentes del Instituto durante la vigencia del contrato, así como incluir al personal y soluciones tecnológicas suficientes para la entrega del servicio.

El **LICITANTE** deberá sujetarse e integrarse con los procesos y soluciones tecnológicas que el Instituto establezca en su modelo de operación para la gestión de TI.

El **LICITANTE** deberá establecer ciclos evolutivos de mejora operativa que aporten al cumplimiento de los niveles de servicio descritos en el presente anexo técnico.

4.2.1.1. Gestión de Servicios

A continuación, se definen los conceptos y las características que de manera enunciativa más no limitativa deben cumplir los procesos que implemente y opere el **LICITANTE** durante la vigencia del servicio.

4.2.1.1.1. Gestión de Eventos

Se entenderá como "evento" todo cambio de estado significativo de un elemento de configuración, BCF, BCC o componente tecnológico, que pueda afectar de manera negativa la prestación del servicio al Instituto, en términos de degradación, desempeño o inclusive denegación.

El **LICITANTE** debe establecer los mecanismos necesarios para detectar eventos que ocurran en los BCFs, BCCs y en cualquier componente tecnológico, su interpretación, notificación y acciones de control que apliquen para su recuperación, así mismo, los eventos podrán indicar que alguna aplicación, servicio o componente no está funcionando correctamente mediante el registro de un incidente a través del proceso descrito más adelante; también pueden indicar una actividad anormal, o la necesidad de una intervención de rutina. Además de indicar el alcance de umbrales operativos.

Los eventos deberán comunicar información operacional a otros procesos de gestión como incidentes, cambios y problemas.

La gestión de eventos deberá operar en un horario 7x24x365 a partir de su implementación y hasta el término del Contrato. Para tal efecto el **LICITANTE** deberá considerar la cantidad de estaciones (agentes más terminales de monitoreo) necesarias para cubrir el horario antes definido.

Este servicio tiene como objetivo conocer la salud de los BCF y los BCC de los servicios tecnológicos asociados al presente anexo técnico, mismo que deberán dar visibilidad al equipo que gestiona el servicio de parte del Instituto.

El servicio deberá hacer énfasis en todo momento a la proactividad, es decir, deberá tener la capacidad de poder identificar anticipadamente una posible falla en cualquiera de los componentes de los bloques de construcción o servicios del presente anexo técnico, notificando mediante alertas a las áreas correspondientes para que se tomen acciones antes de que un evento se materialice en un incidente.

El **LICITANTE** en el monitoreo proactivo deberá considerar, la identificación de los BCF, métricas adecuadas para cada bloque de construcción en el contexto de su implementación, la definición de los umbrales óptimos y sus correlaciones, de alerta y críticos de operación de cada uno de ellos, el seguimiento permanente de los mismos y los esquemas de escalamiento y seguimiento que correspondan a la acción y atención preventiva con el Instituto o los grupos de soporte definidos en las mesas de arranque.

El **LICITANTE** deberá designar un **Coordinador de Eventos**, con los conocimientos y la experiencia necesaria para la administración y seguimiento de este servicio.

El **LICITANTE** como parte de la gestión de eventos, deberá implementar a través de herramientas tecnológicas, la visibilidad a los componentes de la infraestructura, como son los signos vitales (CPU, memoria y acceso a disco), BCF's, BCC y sobre todo las afectaciones colaterales por la degradación del componente, aplicativo o servicio, informando de manera oportuna al Instituto sobre su gestión.

El servicio deberá tener la visibilidad de todos los elementos de configuración (CIs) que formen parte del ecosistema de los servicios que sean transferidos hacia el **LICITANTE**, los cuales deberán estar relacionados de manera ordenada en la **CMDB**.

Actividades enunciativas más no limitativas a cargo del **LICITANTE:**

- Operar la solución tecnológica que permita la visibilidad de los componentes y servicios.
- Detección y filtrado de eventos.
- Registro de eventos en la solución tecnológica
- Correlacionar y dar significado a los eventos
- Seleccionar respuesta y acciones a realizar
- Consultar la Base de Conocimiento
- Acciones de revisión de los componentes y servicios
- Registro de Incidentes por alertamiento de los eventos materializados impactando el servicio.
- Cerrar evento.
- Participar presencialmente en las sesiones de reuniones calendarizadas de parte del Instituto.
- Identificar afectaciones colaterales en servicios que ocupen el componente, aplicación o servicio afectado.

El **LICITANTE** entregara mensualmente el **Reporte de Gestión de Eventos** que incluya de manera enunciativa más no limitativa lo siguiente:

- Número de evento.
- Fecha y hora de apertura del evento.
- Fecha y hora de solución del evento.
- Tiempo de solución del evento.
- Numero de Incidente en caso de derivación al proceso de gestión de incidentes.

4.2.1.1.2. Gestión de Requerimientos

Se entenderá como "requerimiento" a cualquier solicitud parte del Instituto hacia el **LICITANTE** respecto a los servicios relacionados al presente anexo técnico. No se considerarán requerimientos los incidentes, problemas, eventos, modificaciones a la CMDB, ni solicitudes de cambio normales y emergentes.

El **LICITANTE** deberá proporcionar un punto único de entrada para todas las solicitudes que no implican un incidente, tales como accesos, permisos, cambios estándares o requerimientos de información, o cualquier requerimiento relacionado a los servicios del presente anexo técnico, una vez proporcionado y explicado el punto único de entrada, el LICITANTE, deberá llevar un registro documentado de los requerimientos y/o solicitudes.

Actividades a cargo del **LICITANTE**

- Operar la solución tecnológica para la gestión de requerimientos.
- Proporcionar un medio de comunicación para recibir solicitudes del Instituto a través de los canales que éste último establezca.
- Gestionar la solicitud.
- Asegurar la atención de la solicitud.
- Documentar el cierre de la solicitud.

El **LICITANTE** entregará mensualmente el **Reporte de Gestión de Requerimientos** que incluya de manera enunciativa más no limitativa lo siguiente:

- Número de requerimiento.
- Fecha y hora de apertura del requerimiento.
- Fecha y hora de solución del requerimiento.
- Tiempo de solución del requerimiento.
- Información sobre acciones de restauración, diagnóstico y solución del requerimiento.

4.2.1.1.3. Gestión de Incidentes

Se considerará un "incidente" a una interrupción no planificada o reducción en la calidad de un componente, aplicación, servicio o elemento tecnológico descrito en el presente anexo técnico. También será considerado un incidente a la falla de un elemento de configuración, BCF, BCC o plataforma aunque no haya impactado todavía en el servicio.

El proceso deberá restablecer la operación normal del servicio en caso de un incidente tan rápido como sea posible, minimizando el impacto adverso en los componentes, aplicaciones y servicios digitales soportados por el presente anexo.

El impacto y la urgencia deberán estar definidas en la mesas de trabajo de inicio del contrato entre el **LICITANTE** y el Instituto.

Para resolver los incidentes, el **LICITANTE** deberá considerar las prioridades que se establezcan en base al impacto y a la urgencia.

Para la gestión de Incidentes, el **LICITANTE** deberá contar personal especializado en la gestión y deberá coordinarse con los grupos de soporte y gestión que el Instituto determine durante la vida del presente contrato o quien éste señale. El **LICITANTE** deberá designar un **Gestor de Incidentes** quien supervisará el apego al proceso de Gestión de Incidentes, y realizará de acuerdo a este proceso, sugerencias de mejora.

Será considerado un **Incidente Mayor** aquel que deja fuera de operación al menos un servicio crítico del Instituto, algún BCF o BCC que afecte de manera colateral otros servicios o aplicaciones del Instituto, BCF o BCC considerados transversales, Fallas masivas de red, o cualquier servicio que el Instituto haga de conocimiento al **LICITANTE**. El **LICITANTE** deberá establecer, en conjunto con el Instituto, el procedimiento especial para la atención de **Incidentes Mayores** y apegarse a la normatividad vigente del Instituto, que incluya al menos de manera enunciativa más no limitativa: mecanismos de notificación, mecanismos de comunicación, matrices de escalación, grupos de soporte y mesas de trabajo especializadas para la atención de incidentes (WarRooms).

El **LICITANTE** deberá definir los grupos de soporte establecidos y especializados de primer, segundo y tercer nivel de atención.

El **LICITANTE** deberá apegarse a los niveles de escalamiento que se definan en conjunto con el Instituto en las mesas de trabajo durante la vigencia del contrato.

El **LICITANTE** deberá habilitar mecanismos de comunicación agiles (foros sociales, herramientas móviles de comunicación, etc) para el seguimiento de **incidentes (incluyendo los mayores)**, e informar en un resumen final por mecanismos de comunicación formales que el Instituto acuerde con el **LICITANTE** (correo electrónico, postmortems, etc) el resultado de las acciones de solución del Incidente. Estos mecanismos de comunicación formales y agiles, deberán estar aprobados, administrados y supervisados en conjunto con el Instituto y el **LICITANTE**.

El **LICITANTE** deberá entregar, en un plazo no mayor a 72 horas posterior a la solución del incidente, un reporte de análisis **"post-mortem"** de los **incidentes mayores**, o aquellos que el Instituto solicite, así como la propuesta de cálculo de deductiva o penalización por incumplimiento de niveles de servicio, que incluya todos los BCFs y BCCs afectados de manera directa e indirecta. En los reportes post mortem, el **LICITANTE** deberá entregar al menos de manera enunciativa más no limitativa:

- Cronología del Incidente desde su detección, notificación, acciones, grupos participantes, hasta su solución.
- Lista de BCFs, BCCs, afectados de manera directa.

- Componentes, aplicaciones, o servicios afectados colateralmente desglosados en BCFs y BCCs.
- Duración del incidente (detallado por BCF y BCC afectado).
- Acciones de mejora o recomendaciones.

Para la gestión de incidentes el **LICITANTE** efectuará de manera enunciativa más no limitativa, las actividades siguientes:

- Operar la solución tecnológica para la gestión de incidentes.
- Identificar y registrar los incidentes.
- Categorizar, priorizar y realizar diagnóstico inicial.
- Investigar y diagnosticar.
- Solucionar y recuperar.
- Cerrar el incidente.
- Informar al Instituto el estado de los incidentes.

Actividades del **Gestor de Incidentes** del LICITANTE:

- Gestionar el Incidente en conjunto con el Instituto.
- Desarrollar e implementar el proceso.
- Vigilar el cumplimiento y apego al proceso.
- Realizar ajustes y actualizaciones al proceso.
- Desarrollar los indicadores clave de desempeño (KPIs)
- Gestionar el desarrollo de los reporte de indicadores.
- Participar presencialmente en las sesiones de reuniones calendarizadas de parte del Instituto.
- Elaborar el repote postmortem.
- Entregar propuesta de penalización o deductiva.
- Abrir los canales de comunicación necesarios para la atención de incidentes (brigdes telefónicos, foros de comunicación agil, foros móviles etc).

El **LICITANTE** entregará mensualmente el **Reporte de Gestión de Incidentes** que incluya de manera enunciativa más no limitativa lo siguiente:

- Número de incidente.
- Fecha y hora de apertura del incidente.
- Fecha y hora de solución del incidente.
- Tiempo de solución del incidente
- Información sobre acciones de restauración, diagnóstico y solución.
- Servicio afectado.
- Recurrencia de servicios afectados
- BCFs, BCCs afectados de manera directa e indirecta.

4.2.1.1.4. Gestión de Problemas

Se considerará un Problema a una condición identificada en múltiples incidentes que exhiben síntomas comunes y de la cual no se conoce la causa raíz que originó el incidente.

El **LICITANTE** deberá analizar y encontrar la causa raíz que ocasionan eventos e incidentes; realizar actividades proactivas para detectar y prevenir futuros incidentes y definir un subproceso de errores conocidos que permita el diagnóstico de una manera más ágil.

El **LICITANTE** deberá registrar un nuevo problema por uno o varios incidentes recurrentes cuando no exista una solución rutinaria o bien no se conozca la causa raíz que originó la interrupción o degradación en el servicio.

Para la solución de los problemas que se presenten en los servicios descritos en el presente Anexo Técnico, el **LICITANTE** deberá contar con grupos especializados para la atención y diagnóstico de los problemas, conformados por especialistas en las tecnologías descritas en el presente anexo técnico y personal del Instituto.

El **LICITANTE** deberá designar un **Gestor de Problemas** quien se encargará de asegurar el cumplimiento del proceso.

Actividades a cargo del **LICITANTE**

- Operar la solución tecnológica para la gestión de problemas.
- Gestionar la solución de problemas.
- Documentar el problema en conjunto con el Instituto.
- Generar informes del seguimiento del problema.
- Documentar el cierre del problema.

Actividades del **Gestor de Problemas** del **LICITANTE**:

- Organizar, conformar y coordinar los grupos de atención de problemas.
- Ser el enlace con el Instituto para dar seguimiento e informar.
- Ser administrador y resguardar la base de conocimiento de errores conocidos.
- Realizar análisis de casos en la solución tecnológica, principalmente de incidentes y eventos, para detectar problemas.
- Dar seguimiento en la solución tecnológica y registrar errores conocidos.
- Realizar el cierre formal del registro de problemas.
- Ordenar, ejecutar, documentar y dar seguimiento a las actividades relacionadas con la revisión de problemas mayores.
- Generar el plan de trabajo para resolver el problema y dar seguimiento a la ejecución de las actividades.
- Coordinar el registro de los cambios que apliquen, para resolver el problema.
- Generar los indicadores clave de desempeño que correspondan al proceso.
- Realizar el cierre formal del registro de problemas a través de un dictamen.
- Participar presencialmente en las sesiones de reuniones calendarizadas de parte del Instituto.
- Generar el **Dictamen Técnico del problema**

El **LICITANTE** entregará mensualmente el **Reporte de Gestión de Problemas** que incluya de manera enunciativa más no limitativa lo siguiente:

- Número de problema.
- Fecha de apertura del problema.
- Fecha de solución del problema.
- Cantidad de incidentes recurrentes.
- Cambios asociados al problema.
- Acciones realizadas para identificar la causa raíz.
- Incidentes resueltos sin causa raíz detectada.

4.2.1.1.5. Gestión de Cambios

Se considerará un cambio normal cualquier, modificación o eliminación de servicios, elementos de configuración, procesos, documentación, bloque de construcción o relaciones entre componentes en el ecosistema Institucional. Los cambios normales deberá solicitarse mediante un Requerimiento de Cambio (Request for Change RFC) en la solución tecnológica que implemente el **LICITANTE** para la gestión de servicios. Los cambios normales serán sometidos a la aprobación y programación del comité de cambios (Change Advisory Board CAB) que el Instituto señale.

Un cambio estándar es un cambio pre-aprobado por el Instituto, de bajo riesgo, común y sigue un procedimiento o instrucción de trabajo específico. No se solicitarán Requerimientos de Cambios para implementar cambios estándar, pero sí deberán ser registrados y documentados.

Un cambio emergente que deberá ser introducido lo más rápido posible previa autorización obtenida del comité de cambios de emergencia (Emergency Change Advisory Board ECAB) conformado por personal del Instituto y del **LICITANTE**, solo para resolver un incidente mayor y/o un requerimiento de negocio regulatorio. Por lo anterior, un cambio emergente tendrá un procedimiento específico que definirá el Instituto durante las mesas de planeación del arranque y que podrá modificarse durante la vigencia del contrato.

El proceso deberá asegurar que se utilicen métodos y procedimientos estandarizados para el manejo de todos los cambios, optimizando el riesgo total del negocio y reduciendo los incidentes, interrupciones y el re-trabajo.

El **LICITANTE** deberá categorizar los cambios en Normales, Estándar y Emergentes de acuerdo a los criterios que establezca el Instituto en su modelo operativo vigente durante la vigencia del servicio.

El **LICITANTE** deberá planear y organizar los cambios en grupos y secuencia a ejecutarse en días y horarios preestablecidos en común acuerdo con el Instituto, a fin de prevenir afectaciones adversas y realizar validaciones.

Todos los cambios deberán ser registrados en la solución tecnológica que integre la herramienta del instituto con la del **LICITANTE** para la gestión de servicios.

El Gestor de Cambios deberá asegurar que los planes de cambio incluyan todos los elementos para su ejecución, así como los planes de retorno.

El **LICITANTE** deberá designar un **Gestor de Cambios** que será el coordinador y responsable de que todos los cambios se gestionen de acuerdo al proceso que se establezca en conjunto con el Instituto. El Gestor de Cambios será en enlace con el Instituto para los cambios.

Actividades a cargo del **LICITANTE**

- Asegurar que los cambios sean registrados, evaluados, autorizados, priorizados, planeados, probados, implementados, documentados y revisados de una forma controlada.
- Planear y controlar los cambios.
- Participar en la planeación.
- Medir y controlar los cambios.
- Generar información para la toma de decisiones.

- Recibir, registrar y asignar prioridad a todos los RFCs.
- Rechazar los RFC que no se encuentren completos.
- Asesorar en el llenado de los RFC.
- Promover los cambios ante el CAB del Instituto.
- Solicitar ante el ECAB la aprobación de los cambios emergentes.
- Análisis de impacto previo a la ejecución del cambio.
- Participar presencialmente en las sesiones de reuniones calendarizadas de parte del Instituto.

El **LICITANTE** entregará mensualmente el **Reporte de Gestión de Cambios** que incluya de manera enunciativa más no limitativa lo siguiente:

- Número de Requerimientos de Cambio (RFC).
- Duración del Cambio.
- Resultado del Cambio.
- Desviaciones.
- Áreas de oportunidad identificadas.
- Relación de cambios que afectan activos de TI y que deberán de ser actualizados en la CMDB

4.2.1.1.6. Mesa de Servicio

El **LICITANTE** deberá implementar una herramienta de Mesa de Servicios para recibir, registrar, categorizar, dar seguimiento y generar información de los procesos de Gestión de Requerimientos, Gestión de Eventos, Gestión de Incidentes, Gestión de Cambios y Gestión de Problemas, relacionados a los servicios del presente anexo técnico.

A continuación se describen de manera enunciativa más no limitativa, algunos de los eventos que se podrán reportar a la Mesa de Servicio:

- Fallas de hardware en los servidores suministrados al Instituto.
- Degradación de servicio en las aplicaciones o servicios del Instituto.
- Fallas de funcionamiento en Sistema Operativo.
- Fallas de funcionamiento en Bases de Datos.
- Fallas en el software de monitoreo.
- Fallas y/o degradación en los servicios de comunicaciones, por ejemplo, en el enlace LAN to LAN.

El **LICITANTE** deberá categorizar y asignar en tiempo y forma los tickets solicitados por el Instituto, registrando de manera enunciativa más no limitativa:

- Nombre del solicitante.
- Cargo y/o puesto.
- Síntoma.
- Evidencia.
- Servicio afectado.
- Número y correo electrónico para validación de confidencialidad
- Grupos de soporte

El **LICITANTE**, deberá considerar todo lo necesario para llevar a cabo la Integración con la Mesa de Servicios Tecnológicos del Instituto, así como los desarrollos, personal especializado y demás herramientas necesarias para llevarlo a cabo, sin costo adicional para el Instituto.

La Mesa de Servicio deberá estar disponible para atender y gestionar los tickets en un horario de servicio 7x24x365. El **LICITANTE** será responsable de contar con los agentes necesarios para atender la demanda en los diferentes turnos.

Los tickets generados por la Mesa de Ayuda deberán ser despachados hacia los grupos de soporte establecidos por categorización, cuidando en todo momento lo siguiente:

- La Mesa de Servicio debe proporcionar el primer soporte (nivel 1) para la atención inmediatamente del ticket.
- La Mesa de Servicio debe dar seguimiento de inicio a fin para la resolución y/o atención del ticket, pasando por cualquier área de soporte dentro de los niveles: N2 y N3.
- El número de ticket se deberá proporcionar en todos los casos a la persona que solicitó el ticket, cualquier omisión del número de ticket, se considerará como un ticket fallido.
- Todos los tickets deberán registrar el horario en que sean creados.
- Los tickets deberán ser cerrados hasta que el incidente, evento o requerimiento, haya sido solucionado por completo y confirmado por la persona que levantó el ticket, por cualquiera de los canales que habilite la mesa, siempre y cuando genere evidencia de la confirmación del usuario.

El **LICITANTE** entregará mensualmente el **Reporte de Tickets Generados** que incluya de manera enunciativa más no limitativa lo siguiente

- Número de ticket: incidente, problema, evento, requerimiento.
- Fecha de apertura.
- Fecha de solución.
- Tiempo de solución.
- Comentarios de solución.
- Niveles de servicio de ticket.

4.2.1.2. Gestión de Soporte a la Operación

4.2.1.2.1. Administración de Sistemas Operativos

La administración de sistemas operativos contempla la gestión, instalación, configuración, actualización, mantenimiento, soporte, así como la ejecución y documentación de configuraciones de los sistemas operativos, sus componentes y/o subsistemas instalados en equipos físicos y virtuales, salvo aquellos casos que a petición del Instituto la administración del sistema operativo sea compartida con el **LICITANTE** durante un período de transición que se establezca por acuerdo entre ambas partes.

A continuación, se señalan de manera enunciativa más no limitativa las actividades de administración y soporte de sistemas operativos que llevará a cabo el **LICITANTE** dentro del alcance de los servicios del presente Anexo Técnico:

a) El **LICITANTE** será responsable de las actividades de administración de los sistemas operativos que les sean señalados y/o transferidos por parte del Instituto; considerando para dicha operación la aplicación de los procedimientos que sean necesarios para cumplir con las actividades que establece el Proceso de

Administración de la Operación (AOP) del MAAGTICSI vigente; para lo cual deberá desarrollar, implementar y mantener disponibles para su consulta y actualización electrónica, los documentos, herramientas y registros que permitan verificar su cumplimiento (Ejemplo: Mecanismos de Operación, Programas de Tareas, Bitácoras de Operación, etc.).

b) El **LICITANTE** será responsable de la administración, configuración y soporte de los sistemas operativos componentes y/o subsistemas definidos dentro del alcance del servicio, salvo en los casos en que deban ser gestionados de manera total o parcial por otras áreas operativas del Instituto, o por Proveedores de contratos que tenga el Instituto. El **LICITANTE** trabajará con el Instituto para validar la correcta administración y desempeño de dichos sistemas operativos, así como para planear y coordinar las acciones que se requiera que se ejecuten de manera conjunta.

c) El **LICITANTE** será responsable de la atención y/o canalización al área operativa correspondiente de los incidentes y problemas asociados a los sistemas operativos, componentes y/o subsistemas asociados de los equipos dentro del alcance del servicio, mediante el Proceso de Gestión de Incidentes y/o Problemas del Instituto, alineados al MAAGTICSI vigente.

d) El **LICITANTE** comunicará y coordinará a través del Proceso de Gestión de Cambios del Instituto aquellos cambios planeados en las funcionalidades, actualizaciones y mantenimientos a los sistemas operativos, sus componentes y/o subsistemas. El **LICITANTE** previamente revisará y analizará las solicitudes de cambio dentro del alcance de este servicio para dar a conocer al Instituto (a través de la Mesa de Cambios Institucional) el impacto o posibles riesgos que dicho cambio implique con la finalidad de aportar elementos técnicos para evaluar si procede o no su ejecución.

e) El **LICITANTE** será responsable de levantar los casos de soporte directamente a los diferentes fabricantes del sistema operativo, sus componentes y/o subsistemas en caso de falla de producto, así como el seguimiento correspondiente. Dada la diversidad de entornos que el Instituto utiliza en su operación, el **LICITANTE** deberá contar con el personal y los recursos necesarios para el registro, seguimiento y cierre de los casos de soporte con el fin de garantizar la continuidad de la operación. El **LICITANTE** se apegará al mecanismo que el fabricante tenga definido para el levantamiento de un reporte, actualizando el estado en el que se encuentran.

i) En los casos que sea requerido por el Instituto, el **LICITANTE** será responsable de la creación, conversión y/o migración de ambientes de procesamiento virtual a físico, físico a virtual o virtual a virtual, contenedores (incluyendo todos sus componentes instalados: base de datos, middleware, aplicaciones), entre cualquiera de los centros de datos que utiliza el Instituto (incluyendo servicios en la nube); mediante el uso de los diferentes componentes de software de Virtualización que defina y/o integre el Instituto, Asimismo, deberá realizar la creación y administración de plantillas (Templates) que se requieran de dichos ambientes.

j) El **LICITANTE** administrará de manera consistente los parámetros de configuración del sistema operativo, sus componentes y/o subsistemas, a fin de garantizar la continuidad de la operación. En los casos en los que, por disposición del Instituto éstas funciones recaigan en otras áreas operativas del Instituto, el **LICITANTE** tendrá la obligación de validar el correcto funcionamiento del sistema operativo y reportar al Instituto, cualquier incidente o problema que impida o limite el desempeño del sistema operativo, sus componentes y/o subsistemas. El **LICITANTE** dirigirá y coordinará todas las acciones de planeación y

ejecución con otras áreas operativas y/o terceros que se requiera para garantizar el correcto funcionamiento del sistema operativo, sus componentes y/o subsistemas.

k) El **LICITANTE** vigilará y mantendrá activas y vigentes las cuentas administrativas y operativas del sistema operativo, sus componentes y/o subsistemas en los ambientes soportados y definidos dentro del alcance del servicio con el fin de evitar que éstas expiren e impacten negativamente en la operación, si esto último ocurre.

l) El **LICITANTE** realizará un análisis de la situación actual de la configuración de los servidores con el equipo sincronizador de tiempo, con la finalidad de que desarrolle, coordine, implemente y ejecute un plan de trabajo para mantener sincronizados todos los equipos del Instituto, si es necesario, deberá coordinar a las áreas internas del Instituto y a los terceros involucrados. Una vez implementado el plan de trabajo, el **LICITANTE** vigilará y monitoreará la correcta sincronización de los servidores conforme al tiempo.

m) El **LICITANTE** ejecutará scripts en los servidores, siempre y cuando sean solicitados a través del Proceso de Gestión de Cambios del Instituto. Asimismo, el **LICITANTE** previamente revisará y analizará dichos scripts para que dé a conocer al Comité de Aceptación de Cambios (CAB) el impacto y/o posibles riesgos que implica la ejecución de dichos scripts, lo anterior con la finalidad de evaluar si es que procede o no la ejecución de estos.

4.2.1.2.2. Administración de Base de Datos

El **LICITANTE** será responsable de la administración y soporte de las Bases de Datos, manejadores, instancias, así como el software relacionado, tales como: DB2, Oracle, SQL, PostgreSQL, mongo DB, entre otros que defina el Instituto durante la vida del contrato, en cualquiera de los ambientes soportados por el presente anexo técnico.

La administración y soporte de las Bases de Datos, manejadores, instancias, y software relacionado incluye todas las actividades requeridas y/o necesarias para su correcta operación.

A continuación, se señalan de manera enunciativa más no limitativa las actividades de administración y soporte de las Bases de Datos, instancias, y software relacionado que llevará a cabo el **LICITANTE** dentro del alcance de los servicios del presente Anexo Técnico:

a) El **LICITANTE** será responsable de la administración, configuración y soporte de las Bases de Datos, manejador de Bases de Datos, instancias, y software relacionado.

b) El **LICITANTE** será responsable de realizar las altas, bajas y cambios de las Bases de Datos, los manejadores de Bases de Datos, instancias, y software relacionado a través del Proceso de Gestión de Cambios.

c) El **LICITANTE** será responsable de la resolución de incidentes y problemas asociados a las Bases de Datos, instancias, y software relacionado mediante los Procesos de Gestión de Incidentes y Gestión de Problemas definidos en el presente Anexo Técnico.

d) El **LICITANTE** comunicará y coordinará a través del Proceso de Gestión de Cambios del Instituto aquellos cambios planeados, previamente revisará y analizará las solicitudes de cambio dentro del alcance de este servicio para dar a conocer al Instituto el impacto o posibles riesgos que dicho cambio implique con la finalidad de evaluar si procede o no su ejecución. Asimismo, deberá involucrar a los diferentes grupos de Soporte (Aplicaciones, Redes, Almacenamiento, Sistemas Operativos, entre otros que defina el Instituto) y terceros involucrados.

e) Derivado de una recomendación, valoración, incidente, problema y/o propuesta de un tercero, el **LICITANTE** mediante las mejores prácticas será responsable de analizar, medir el impacto y riesgo operativo, desarrollar un plan de trabajo, coordinarse con terceros y ejecutar las acciones derivadas mediante el Proceso de Gestión de Cambios del Instituto.

f) El **LICITANTE** definirá y/o ejecutará los requerimientos de configuración del manejador de bases de datos (instancias). Asimismo, deberá coadyuvar a la tropicalización con las áreas internas y/o con los terceros involucrados; entiéndase como tropicalización la configuración adecuada del manejador con los ambientes propios del Instituto.

h) El **LICITANTE** ejecutará los requerimientos de homologación de configuraciones de las Bases de Datos, instancias, objetos y software relacionado para los diferentes ambientes. El **LICITANTE** mantendrá consistencia entre los parámetros de todas las Bases de Datos que están directamente asociados a un tamaño o plataforma cuando éstas sean similares.

i) En los casos que sea requerido por el Instituto, el **LICITANTE** será responsable de la migración de Bases de Datos a otro ambiente al que se encuentre actualmente y dentro del alcance de este servicio.

j) El **LICITANTE** deberá instalar y proveer las herramientas que le permitan automatizar las tareas de administración, generación, modificación, monitoreo y soporte de las Bases de Datos.

k) En caso de presentarse una falla técnica del producto en los diferentes manejadores, el soporte técnico será provisto por el fabricante siempre y cuando la versión este soportada, para lo cual el Instituto contará con los contratos de cada uno de los productos que se encuentren en operación. En caso de requerir apoyo del fabricante, el LICITANTE deberá interactuar, escalar y coordinar con el fabricante, sí y sólo si, el producto tiene un defecto.

l) El **LICITANTE** se apegará al mecanismo que el fabricante tenga definido para el levantamiento de un reporte, notificando al GGC del estado del reporte.

m) El **LICITANTE** contemplará un servicio de soporte de tercer nivel en productos Oracle, quien llevará a cabo entre otras actividades que defina el Instituto:

a. Levantamiento de casos de soporte con el fabricante del producto.
b. La capacidad de identificar y entregar reportes de causa raíz validados por el fabricante.
c. Contar con herramientas de soporte que permitan asistir en la recolección de información y evidencias técnicas más allá de la información que emita la plataforma de monitoreo permitiendo acelerar el análisis de un incidente.

o) El **LICITANTE** con el fin de evitar la degradación en el rendimiento de los equipos será responsable de validar que al menos las bases de datos estén excluidas del escaneo del antivirus institucional instalado en los servidores y/o cualquier recomendación del fabricante que provoquen una degradación.

q) El **LICITANTE** administrará de manera consistente los parámetros de configuración del manejador de Base de Datos a fin de garantizar la continuidad de la operación.

q) El **LICITANTE** vigilará y mantendrá activas y vigentes las cuentas administrativas y operativas de Bases de Datos, de los ambientes soportados y bajo las políticas definidas por el servicio de gestión de seguridad de la información, dentro del alcance del servicio con el fin de evitar que éstas expiren e impacten negativamente en la operación.

r) El **LICITANTE** ejecutará scripts en los servidores del Instituto, siempre y cuando sean solicitados a través del Proceso de Gestión de Cambios y se tenga el visto bueno de las áreas de Seguridad de la Información del Instituto cuando así aplique. Asimismo, el **LICITANTE** previamente revisará y analizará los scripts para que dé a conocer al Grupo de Gobierno del Contrato el impacto o posibles riesgos que implica la ejecución de dichos scripts, lo anterior con la finalidad de evaluar si es que procede o no la ejecución de estos.

4.2.1.2.3. Administración y Soporte del Middleware

El Middleware es un software intermedio que ofrece un conjunto de servicios que hacen posible el funcionamiento de las Aplicaciones (incluyendo en algunos casos, productos de replicación de datos), distribuidas sobre plataformas heterogéneas; que se sitúa entre las capas de aplicaciones y las capas inferiores como Base de Datos, Sistema Operativo y Red.

El Middleware ofrece servicios de infraestructura de software para que las Aplicaciones, puedan operar sobre una plataforma tecnológica e intercambiar datos entre éstas. Esto incluye servidores web, servidores de Aplicaciones, productos de replicación de datos, sistemas de gestión de contenido y herramientas similares utilizando tecnologías como XML, SOAP, servicios web y arquitecturas orientadas a servicios (SOA), entre otras que defina el Instituto.

Los componentes Middleware se distinguen de Aplicaciones finales y de servicios de plataformas específicas por cuatro importantes propiedades:

1. Son independientes de las Aplicaciones para las que éstas se desarrollan.
2. Se pueden ejecutar en múltiples plataformas.
3. Se encuentran distribuidos.
4. Soportan interfaces y protocolos estándar.

El alcance del servicio Middleware contempla la instalación, reinstalación, administración, soporte, configuración, puesta a ppunto, afinación, mantenimiento, respaldos, licenciamiento y versionamiento, actualizaciones, seguridad operacional y lógica, gestión, ejecución y documentación de la configuración de sus componentes; instalados en equipos físicos y virtuales en los ambientes dentro del alcance de este servicio y que no sean administrados por otros contratos y/o áreas operativas del Instituto.

Asimismo, el **LICITANTE** identificará y notificará al Instituto aquellos procesos, tareas, comandos, manuales que sean susceptibles de automatización a través de programas, shells, Scripts, etc. a fin de ejecutar acciones diarias de operación, eliminando así posibles errores humanos para llevar a cabo de manera eficiente la administración y soporte del Middleware.

A continuación, se señalan de manera enunciativa más no limitativa las actividades de administración y soporte que llevará a cabo el **LICITANTE** dentro del alcance del servicio.

a) Planear, organizar, dirigir y controlar las actividades necesarias que garanticen el óptimo funcionamiento del Middleware dentro del alcance de los servicios del presente Anexo Técnico, y a las que el Instituto determine durante el tiempo de vida del contrato; la instalación, reinstalación, administración, soporte, configuración, Tuning, mantenimiento, respaldos, apoyo al GGC del presente Anexo Técnico en la administración del licenciamiento provisto por los contratos vigentes del Instituto; así como su versionamiento, actualizaciones, seguridad operacional y lógica, gestión, ejecución y documentación de la configuración de sus componentes; instalados en equipos físicos y virtuales en los ambientes soportados.

b) El **LICITANTE** será responsable del soporte del Middleware garantizando la correcta y óptima operación del mismo, durante y a lo largo del tiempo de vida del proyecto aplicando las mejores prácticas de TI. Esto incluye la solución de incidentes, problemas y, en su caso, escalación con el soporte técnico del fabricante (soporte de tercer nivel) y las facultades que le serán otorgadas al **LICITANTE** para que cuente con los accesos requeridos a los sitios del fabricante del Middleware a fin de contar con información actualizada. Dichos accesos serán proporcionados por el Instituto de acuerdo con los contratos que tenga definidos con el (los) fabricante(s).

c) El **LICITANTE** será responsable de la atención de incidentes y problemas asociados al Middleware de los equipos dentro del alcance de este servicio, mediante el Proceso de Gestión de Incidentes y/o Gestión de Problemas establecidos en este documento.

d) El **LICITANTE** comunicará y coordinará a través del Proceso de Gestión de Cambios del Instituto aquellos cambios planeados en las funcionalidades, actualizaciones y mantenimientos del Middleware. El LICITANTE previamente revisará y analizará las solicitudes de cambio dentro del alcance de este servicio para dar a conocer al Instituto el impacto o posibles riesgos que dicho cambio implique con la finalidad de evaluar si procede o no su ejecución.

e) El **LICITANTE** será responsable de levantar los casos de soporte directamente a los diferentes fabricantes del middleware en caso de falla de producto, así como de dar el seguimiento correspondiente.

f) El **LICITANTE** contemplará un servicio de soporte de tercer nivel en productos Oracle, certificado por el mismo fabricante, quien llevará a cabo, entre otras actividades que defina el Instituto:

a) Levantamiento de casos de soporte con el fabricante del producto

b) La capacidad de identificar y entregar reportes de causa raíz validados por el fabricante

c) Contar con herramientas de soporte que permitan asistir en la recolección de información y evidencias técnicas más allá de la información que emita la plataforma de monitoreo permitiendo acelerar el análisis de un incidente.

i) El **LICITANTE** administrará de manera consistente los parámetros de configuración y afinación (Tuning) del Middleware a fin de garantizar la continuidad de la operación.

j) En los casos que sea requerido por el Instituto, el **LICITANTE** será responsable de la migración de Middleware a otro ambiente al que se encuentre actualmente.

4.2.1.2.4. Instalaciones de Software

I. Instalación

a) El **LICITANTE** será responsable de la habilitación, instalación, configuración y puesta a punto de los Sistema Operativo, Base de Datos, Middleware y cualquier otro componente tecnológico dentro del alcance del servicio del presente Anexo Técnico.

b) El **LICITANTE** participará en la planeación y coordinación de la instalación, configuración de Sistema Operativo, Bases de Datos, Middleware y cualquier otro componente tecnológico relacionado con los servicios del presente Anexo Técnico a través del Proceso de Gestión de Cambios. Asimismo, deberá proveer soporte durante el desarrollo de actividades que ejecuten las áreas operativas del Instituto o a través de terceros involucrados relacionados con los servicios del presente Anexo Técnico.

c) El **LICITANTE** será responsable de realizar (o de brindar acceso con privilegios a un usuario autorizado) la instalación y/o configuración de productos de software adicional y/o productos de terceros que le requiera el Instituto (compiladores, bibliotecas, web servers, binarios, etc.) a nivel Sistema Operativo, Bases de Datos, Middleware y cualquier otro componente tecnológico. El **LICITANTE** recibirá una guía de Instalación o configuración para los productos de terceros en los casos donde sea necesario.

d) En todos los casos que aplique y sea necesario, el **LICITANTE** deberá considerar y aplicar configuraciones certificadas del fabricante del producto, o por un tercero certificado por éste, como parte de sus responsabilidades.

II. Reinstalación

a) El **LICITANTE** es responsable de la reinstalación o restauración de un ambiente entregado vía el protocolo entrega recepción hacia la operación con todos sus componentes de Software instalados cuando se diagnostique y/o se concluya una falta de alternativa de solución para solventar un incidente, problema o por una afectación al Sistema Operativo, Base de Datos, Middleware, así como a petición del Instituto indistintamente del nivel de protección de Hardware que se tenga.

b) Para cumplir con el inciso anterior, el **LICITANTE** gestionará la instalación del Sistema Operativo en su configuración básica que cumpla con las características necesarias para dicha restauración; y a partir de este punto, el **LICITANTE** continuará con las instalaciones y/o configuraciones necesarias hasta dejar el ambiente operando como se encontraba originalmente en todas sus capas, documentando todo lo anterior a través del Proceso de Gestión de Cambios.

c) El **LICITANTE** será responsable de establecer los mecanismos y alcances de respaldo necesarios (respaldo completo, File System, configuración, entre otros que defina el Instituto) que le permitan restaurar un servidor cuando el **LICITANTE** lo requiera, ya sea por un incidente, un problema u otra causa; o bien, por requerimiento del Instituto.

d) El **LICITANTE** será responsable de restaurar Bases de Datos que tenga bajo su administración, cuando diagnostique y/o pronuncie una falta de alternativa de solución para solventar un incidente o problema o cuando el Instituto así lo requiera, basándonos en la política de respaldo del instituto.

e) El **LICITANTE** deberá considerar y aplicar configuraciones certificadas del fabricante del producto, o por un tercero certificado por éste, como parte de sus responsabilidades.

4.2.1.2.5. Actualizaciones de Software

El **LICITANTE** será responsable de las actualizaciones a las versiones del Sistema Operativo, Bases de Datos, Middleware y cualquier componente de software necesarios para su funcionamiento, así como las configuraciones adecuadas derivadas de recomendaciones de terceros, a solicitud del Instituto o requeridas por la operación, con apego a las mejores prácticas de TI. Para los casos en las que dicha actualización deba ser ejecutada por otras áreas operativas del Instituto, el **LICITANTE** será responsable de validar la correcta instalación y/o actualización del Sistema Operativo, Bases de Datos, Middleware y cualquier componente de software, así como de notificar puntualmente a las áreas correspondientes del Instituto a través del GGC, sobre cualquier riesgo o impacto negativo provocado por la instalación de otras áreas operativas o terceros involucrados.

Para lograr esto, el **LICITANTE** analizará, planeará y coordinará los esfuerzos de las áreas necesarias dentro de su organización, con las áreas internas del Instituto y con los terceros involucrados hasta su conclusión.

El **LICITANTE** será responsable de descargar actualizaciones de las versiones del Sistema Operativo, Bases de Datos y Middleware, con el fin de planear y ejecutar su implantación a través del Proceso de Gestión de Cambios del Instituto. En caso de no tener privilegios de descarga, el **LICITANTE** solicitará dichas actualizaciones a través del Grupo de Gobierno del Contrato para que le sean entregadas por otro medio para su instalación.

El **LICITANTE** realizará las actividades de coordinación, planeación, copiado, movimiento, replicación, migración, clonación y/o ejecución de la actualización de la configuración y/o restaurar la información del File System del Sistema Operativo, componentes y/o subsistemas relacionados entre los ambientes que el

Instituto establezca, por requerimiento específico o a partir de la configuración que se necesite para los ambientes soportados, cumpliendo con los lineamientos del área de Seguridad de la Información donde aplique. En caso de las acciones antes mencionadas deban ser ejecutadas por otras áreas operativas o terceros involucrados, el **LICITANTE** en conjunto con el GGC definirán las acciones de planeación, coordinación y validación de cualquier actividad encaminada a la actualización de la configuración y/o restauración de File System de Sistema Operativo y componentes y/o subsistemas relacionados.

El **LICITANTE** será el encargado de designar responsables de la gestión y seguimiento de las actividades de instalación y/o actualización, y contar con los recursos necesarios para atender todas las actualizaciones que se requieran en los ambientes soportados.

4.2.1.2.6. Administración de la Seguridad en la Operación

Con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información, se requiere que se establezcan los siguientes niveles de seguridad por parte del **LICITANTE**, sobre los ambientes dentro del alcance del presente Anexo Técnico y cuya implementación no afecte de forma negativa, genere conflicto, impida o limite las actividades que se espera que el **LICITANTE** realice sobre los servicios tecnológicos, sin que éstos sean limitativos. Para lo anterior el Servicio de Continuidad Operativa atenderá y se apegará a lo que emita en políticas el Sistema de Gestión de Seguridad de Información del servicio de Seguridad.

I. Seguridad Lógica

a) Verificación de Controles de Seguridad.

Con base en el Sistema de Gestión de Seguridad de Información (SGSI), el **LICITANTE** será responsable de la generación y seguimiento de un plan de trabajo orientado a garantizar la correcta implantación de controles de seguridad comprendidos en el Sistema Operativo que garanticen la integridad de los ambientes. Este plan de trabajo deberá ser revisado y aprobado por el grupo de Gobierno del Contrato y el área de Seguridad de la Información del Instituto.

b) Políticas de Seguridad Institucionales.

El **LICITANTE** será responsable de cumplir y aplicar las configuraciones y/o políticas específicas solicitadas por las áreas de Seguridad de la Información del Instituto y de coordinar y dar continuidad a los proyectos que ésta tenga en desarrollo, orientados a reducir las vulnerabilidades y disminuir los riesgos de seguridad de los ambientes. Con este fin, el **LICITANTE** proporcionará, a solicitud del Instituto.

d) Auditoría de archivos de historial (Log de Sistemas Operativos).

El **LICITANTE** será responsable de realizar una revisión continua de los eventos históricos almacenados en los archivos tipo "Log" para evaluar, gestionar y notificar con oportunidad sobre la detección de un riesgo en el sistema, acompañado de un plan de acción para solventarlo mediante el Proceso de Gestión de Cambios del Instituto. Asimismo, deberá asegurar el resguardo histórico de dichos Logs por el tiempo y volumetría que sea acordado con el Instituto, tiempo que podrá ser actualizado mediante acuerdo formalizado para atender

las necesidades de la operación. Adicionalmente, se tendrá que mantener un registro electrónico de los riesgos detectados y las actividades realizadas en cada uno de ellos.

En caso de impactos negativos en los ambientes del Instituto, derivados de la omisión de esta revisión, se aplicarán las deductivas correspondientes establecidas en la Sección denominada "Penalizaciones y Deducciones al Pago" correspondiente a la presente convocatoria.

e) Auditoría de cumplimiento normativo:

El **LICITANTE** será responsable de realizar una revisión continua del cumplimiento normativo de lineamientos de configuración de seguridad; mediante una herramienta para análisis de vulnerabilidades que les permita escanear los componentes de infraestructura dentro del alcance del servicio; incluyendo la funcionalidad de implementar políticas de seguridad e identificar aquellos equipos que no cumplan con las mismas; la generación y seguimiento de reportes de vulnerabilidades en diferentes formatos comunes (PDF, CSV, XLS, etc.); la clasificación de las vulnerabilidades y riesgos en varios niveles de criticidad (considerando al menos los niveles bajo, medio, alto y crítico). El resultado de los análisis de vulnerabilidades será compartido por el área de seguridad del LICITANTE hacia el Instituto.

II. Seguridad Operacional

a) El **LICITANTE** administrará y garantizará que todas las cuentas de usuario generadas en los servidores se apeguen a las políticas de normatividad establecidas por el área de Seguridad del Instituto.

b) El **LICITANTE** implementará las herramientas y procesos que le permitan notificar al Instituto los incidentes de violación a cualquier política de seguridad, misma que deberá reportarse inmediatamente al Grupo de Gobierno del contrato y al área de Seguridad de la Información del Instituto, conforme a la Matriz de Escalamiento de la Operación del Servicio presentada como parte integral del Programa de Trabajo detallado correspondiente al servicio.

El área de Seguridad de la Información del Instituto será responsable de la definición de las políticas a que debe apegarse el **LICITANTE**; misma que vigilará su cumplimiento de manera aleatoria, como parte de la gestión y soporte del servicio dentro del alcance del contrato. Es importante mencionar que las actividades de vigilancia que realice el **LICITANTE** dentro del alcance del presente Anexo Técnico, se consideran un ejercicio complementario a cualquier otro servicio especializado de seguridad que se utilice en el Instituto, con el fin de contar con un mayor control y seguridad de la información.

c) El **LICITANTE** implementará y/o administrará las herramientas que le permitan la medición de contención y bloqueo de amenazas bajo los lineamientos que dicte el área de Seguridad de la Información del Instituto. Los lineamientos de seguridad referentes a los elementos de procesamiento deberán ser acatados por el **LICITANTE**, quien estará obligado a la revisión y validación de las herramientas de seguridad necesarias. El **LICITANTE**, en conjunto con el Grupo de Gobierno del contrato y el área correspondiente de Seguridad de la Información, deberá observar la correcta instalación de dichas herramientas; incluso cuando éstas sean instaladas por otras áreas operativas del Instituto administradas por diferentes contratos.

d) El **LICITANTE** acordará e informará de la caducidad o vigencia de los certificados de seguridad instalados en los ambientes soportados, 90 días naturales antes de dicho vencimiento. Para ello deberá administrar y gestionar estos certificados mediante un procedimiento acordado en conjunto con el área que el Instituto asigne o un tercero a través de ésta.

e) El **LICITANTE** contemplará que el Instituto podrá requerir la interacción con otros contratos de seguridad que existan durante la vida del contrato, para lo cual se establecerán acuerdos de niveles de operación (OLA´s) entre los mismos para el intercambio de información o servicios.

4.2.1.2.7. Control del Licenciamiento y Versionamiento

- **Licenciamiento**

El **LICITANTE**, deberá mantener un control del licenciamiento en la asignación y utilización de las licencias asignadas al Sistema Operativo. Para lo anterior el Instituto debe proporcionar un listado con la relación de licencias con las que cuenta. El **LICITANTE** avisará al Gobierno del Contrato 3 meses antes del vencimiento de las licencias.

- **Versionamiento**

El **LICITANTE** entregará un análisis de la situación actual de las versiones del Sistema Operativo, con el fin de identificar aquellas que estén próximas a salir o se encuentren fuera de soporte por parte de los fabricantes, permitiendo tomar acciones preventivas que garanticen la continuidad de la operación del Instituto.

Con base en el análisis entregado, el **LICITANTE** será responsable de la generación y seguimiento de un plan de trabajo orientado a garantizar la correcta actualización de las versiones del Sistema Operativo, Bases de Datos y Middleware dentro de los ambientes. Dicho plan deberá ser integrado en el mes que se haya actualizado y acordado con el Instituto.

El **LICITANTE** será responsable de revisar de manera continua, las versiones de los productos instalados en los diferentes ambientes soportados para dar aviso oportuno al Gobierno de Contrato del presente Anexo Técnico, 3 meses antes de la caducidad del producto y se puedan tomar las medidas pertinentes, con el fin de garantizar la vigencia del Sistema Operativo, Bases de Datos y Middleware utilizados por el Instituto.

El **LICITANTE** será designará un **Coordinador de Licenciamiento y Versionamiento**, encargado de la gestión y seguimiento de las actividades de control y actualización de las versiones en uso, y contar con los recursos necesarios para mantener el control del licenciamiento y versionamiento en los ambientes soportados por el presente anexo técnico.

4.2.1.2.8. Afinación (Tuning)

Con un enfoque proactivo, durante la vida del proyecto y de manera periódica, el **LICITANTE** será responsable de identificar, analizar, proponer y ejecutar las tareas de optimización de configuraciones necesarias para el procesamiento, componentes y/o subsistemas que le permitan lograr los niveles de servicio establecidos por el Instituto. La Afinación se deberá realizar en todos los ambientes del Instituto, a través de un plan de trabajo que será integrado, en el mes que se haya ejecutado para su seguimiento y control.

El **LICITANTE** será responsable de evaluar, analizar y corregir problemas de desempeño ocasionados por fallas del Sistema Operativo, Bases de Datos y Middleware y/o algún otro elemento de configuración de hardware o software (Middleware, Aplicaciones, entre otros que defina el Instituto) hasta donde el Sistema Operativo permite y agote su afinación.

El **LICITANTE** será responsable de la gestión y seguimiento de las actividades de las actividades de afinación y contar con los recursos necesarios dentro del alcance de este servicio.

4.2.1.2.9. Consolidación Tecnológica

Con el fin de cumplir con los objetivos de optimización de recursos, simplificación de procesos, reducción de costos y mitigación de riesgos de operación, el **LICITANTE** realizará un plan de trabajo con base en el inventario inicial para analizar los elementos tecnológicos actuales, evaluar alternativas y elaborar los planes de trabajo destinados a la consolidación de la infraestructura, con el fin de lograr durante la vida del contrato, una meta acordada y formalizada con el Instituto, a través del Grupo de Gobierno del Contrato para la reducción en la cantidad de procesadores utilizados respecto del inventario inicial, así como la optimización de licenciamiento, en aquellos equipos físicos que decida el cliente migrar a plataformas de virtualización.

Adicionalmente, el **LICITANTE** incluirá durante la vida del contrato, nuevos objetivos de consolidación tecnológica, conforme a las necesidades de operación del Instituto, mediante un plan de trabajo en paralelo al inventario inicial, para lo cual se acordarán objetivos particulares con el Instituto, a través del Grupo de Gobierno del Contrato del presente Anexo Técnico.

El **LICITANTE** utilizará las herramientas institucionales de Virtualización propias, así como una metodología de trabajo permita maximizar los beneficios para la organización y mitigar los riesgos identificados; hacer uso de prácticas y tecnologías líderes en el mercado; optimizar el soporte operativo y los niveles de servicio para los usuarios finales; definir e implementar la estrategia de consolidación/migración que satisfaga los requerimientos del Instituto; racionalizar el uso de aplicaciones donde sea apropiado; determinar una línea base del desempeño de la infraestructura antes y después de los esfuerzos de consolidación/migración; mantener un nivel de seguridad aceptable en todo momento durante los esfuerzos de consolidación/migración; y comunicar los resultados y avances al órgano de gobierno del contrato.

El **LICITANTE** deberá entregar de manera mensual el ejercicio de consolidación en donde se pueda observar de manera enunciativa más no limitativa elementos tales como: Servidores físicos, capacidades de

procesamiento físico, memoria física, almacenamiento asignado, servidores virtuales, procesamiento virtual, memoria virtual, clasificación (servidor web, servidor de aplicaciones, base de datos, etc), software que utiliza el servidor virtual, licenciamiento, capacidades del host físico (subutilización, sobre utilización), etc. El Instituto en conjunto con el **LICITANTE** acordará el mecanismo de reporte y medición durante las mesas de trabajo iniciales.

El **LICITANTE** en conjunto con el Instituto definirá, vigilará y dará seguimiento a los esfuerzos coordinados de proveedores y áreas del Instituto en la consecución de las metas de consolidación establecidas en el presente Anexo Técnico.

La definición de acuerdos, mecanismos, integraciones de participantes y demás elementos necesarios para el ejercicio de consolidación serán responsabilidad del **LICITANTE** en acuerdo y aprobación por parte del Instituto.

El **LICITANTE** será responsable y encargado de la gestión y seguimiento de las actividades de consolidación dentro del alcance de este servicio, y contar con los recursos necesarios para cumplir con las metas acordadas con el Instituto.

4.2.1.2.10. Mantenimiento de Plataformas

El **LICITANTE** será responsable de ejecutar la gestión y seguimiento de los procedimientos preventivos, actualizaciones y correcciones que se deberán instalar en los ambientes soportados, y contar con los recursos necesarios para coordinar todas las actividades de mantenimiento que se requieran en los ambientes dentro del alcance del servicio.

El **LICITANTE** con el objetivo de que los ambientes del Instituto se mantengan en las mejores condiciones operativas de seguridad y de integridad, se deberán realizar los mantenimientos e instalaciones de acuerdo con los siguientes puntos:

I. Políticas y procedimientos documentados

El **LICITANTE** será responsable de identificar, desarrollar y aplicar las políticas y procedimientos apegados a las mejores prácticas de TI, con el fin de garantizar su continua operación de acuerdo con las características específicas de cada ambiente soportado, como, por ejemplo: reinicios programados, desfragmentación de almacenamiento, depuración de logs, instalación de parches y/o hotfixes, entre otros que defina el Instituto.

II. Calendario

El **LICITANTE** será responsable de proponer y acordar con las áreas correspondientes del Instituto, un calendario de mantenimiento preventivo de los Sistemas Operativos Windows de los ambientes soportados.

III. Desarrollo y ejecución del Plan de Trabajo

El **LICITANTE** será responsable de coordinar e integrar con los terceros involucrados, el plan de trabajo de instalaciones de parches y/o hotfixes, el cual deberá ser aplicado por el **LICITANTE** en los ambientes no administrados por otros contratos. Para tal efecto deberá desarrollar un plan de trabajo gestionado a través del proceso de control de cambios.

IV. **Instalación**

1. Identificación de procedimientos y obtención de parches, hotfixes, entre otros que defina el Instituto, de los distintos fabricantes.

a) Investigación y recomendaciones

El **LICITANTE** será responsable de identificar, relacionar y elaborar una propuesta para la instalación de parches y/o hotfixes que permita llevarlos al último nivel de actualización y/o documentar las excepciones que se encuentren, en todos los ambientes Windows soportados por el **LICITANTE**. Esto lo deberá realizar al menos de manera mensual y en coordinación con las publicaciones efectuadas por los distintos fabricantes y conforme a las mejores prácticas de TI.

b) Acceso y descarga de insumos

El **LICITANTE** será responsable de implementar los mecanismos necesarios y suficientes para garantizar su acceso a las herramientas que los diferentes fabricantes ponen a disposición, con el fin de revisar la documentación, identificar los requerimientos, riesgos y ventajas de la instalación y realizar la descarga de los insumos del software por instalar.

2. **Registro de parches e ingreso al Proceso de Gestión de Cambios**

El **LICITANTE** será responsable de registrar, encolar y/o subir en la herramienta correspondiente del Instituto, el paquete de software que contenga los parches y/o hotfixes a instalar, asegurando su integración con el Proceso de Gestión de Cambios.

a) **Ejecución**

Para los componentes, aplicativos y servicios de negocio en el alcance de este Anexo Técnico, el **LICITANTE**, una vez liberados los paquetes, deberá desarrollar la logística, coordinar y ejecutar la instalación de los mismos, considerando el impacto que ésta pueda tener a través de todas las capas tecnológicas y efectuando las gestiones necesarias solicitadas por el Proceso de Gestión de Cambios. En caso de afectar la operación al instalar parches y/o hotfixes por causa de acciones u omisiones del **LICITANTE**, se aplicarán las deductivas correspondientes en la Sección denominada "Penalizaciones y Deducciones al Pago" correspondiente a la presente anexo técnico.

b) Validación de los parches y hotfixes aplicados

El **LICITANTE** será responsable de verificar la correcta aplicación de los paquetes instalados y el cliente validará la correcta funcionalidad del servicio en los ambientes soportados del Instituto, garantizando una plataforma operativa homogénea.

c) Reportes de parches instalados y procedimientos efectuados en Sistemas Operativos

El **LICITANTE** será responsable de elaborar y mantener un control de las actividades de mantenimiento a los Sistemas Operativos dentro del alcance de los servicios señalados en el presente Anexo Técnico, con el fin de asegurar su adecuado seguimiento y control.

El **LICITANTE** deberá entregar de manera mensual la evidencia documental que soporte las acciones referentes a este apartado, consistentes en todos aquellos reportes, bitácoras, minutas y elementos electrónicos o impresos que comprueben el devengo de los servicios y cumplimiento de las obligaciones descritas en el presente anexo técnico, apéndices anexos, términos y condiciones, oferta del licitante y documentación contractual

4.2.1.2.11. Automatización de Comandos

Como parte de la Administración del **LICITANTE** en los Sistemas Operativos, Bases de Datos y Middleware, el **LICITANTE** identificará los procesos, tareas y comandos que sean susceptibles de automatización (mediante programas, shells, scripts, etc.) para la ejecución de las acciones diarias de operación, eliminando posibles errores humanos y con ello llevar a cabo de manera eficiente la administración de los sistemas operativos.

Aspectos generales del apartado Gestión de Soporte a la Operación

El **LICITANTE** deberá ofertar, detallar, documentar, proporcionar, habilitar, configurar, poner a punto, operar y gestionar la operación e incluir en su propuesta todo lo necesario para dar cumplimiento al rubro de ***Gestión de Soporte a la Operación*** requerido por el Instituto en el presente anexo técnico, apéndices anexos, términos y condiciones, oferta del licitante y documentación contractual.

4.2.1.3. Soluciones Tecnológicas del Centro de Continuidad Operativa

4.2.1.3.1. Visibilidad de los servicios

El **LICITANTE** deberá aprovisionar, implementar, configurar, poner a punto, operar, administrar, soportar y mantener todos los elementos de software, hardware y recursos humanos necesarios, como parte integral del servicio.

La solución tecnológica provista por el **LICITANTE** para este servicio deberá contar con las siguientes funcionalidades, listadas de manera enunciativa más no limitativa:

a) La solución que el **LICITANTE** empleé deberá estar alineada a lo establecido en las mejores prácticas para la operación, basándose en orientación de gestión de servicios.

b) Por cuestiones de interoperabilidad e independencia de la plataforma monitoreada, la herramienta propuesta deberá contemplar el monitoreo sin agentes, a excepción de los casos en los cuales se demuestre la no factibilidad de esta opción o sea una necesitad especifica de profundidad que requiera instalación de agentes, en cuyo caso El **LICITANTE** entregará un reporte técnico que lo sustente.

c) La herramienta de monitoreo propuesta tendrá que integrar la gestión de todos los elementos relacionados e involucrados tanto físicos como lógicos, en los servicios del Instituto, que contemple las siguientes capas enunciativas, más no limitativas:

1. capa de red,
2. capa de presentación,
3. capa de procesamiento,
4. capa de almacenamiento y;
5. capa de base de datos.

d) La solución deberá ser capaz de correlacionar eventos o fallas en el funcionamiento de los diversos elementos que componen todos los servicios del Instituto, para que, en el menor tiempo posible, el personal especializado del **LICITANTE** cuente con elementos para identificar, aislar la causa raíz del evento y ejecute o sugiera acciones para su resolución.

e) El acceso para administración deberá ser mediante interfaz Web a una consola centralizada desde cualquier punto de la red del Instituto. Para lo anterior, se deberán considerar por lo menos 20 licencias de acceso de conexión e infraestructura dedicada con al menos 8 terminales de visualización (pantallas con su respectivo dispositivo de acceso que permitan visualizar las plataformas de monitoreo de los componentes, aplicaciones o servicios) para las áreas de operativas y directivas del Instituto, mismas que serán instaladas donde el Instituto requiera.

f) La solución deberá manejar roles/perfiles de usuarios para definir permisos y tipo de notificación a cada uno.

g) El sistema de monitoreo deberá permitir integración con las soluciones de identidad y control de acceso del Instituto.

h) Permitirá contabilizar el número de veces que llega la misma alarma o evento, con el fin de evitar duplicidades.

i) La herramienta deberá tener la capacidad de funcionar en un esquema de arquitectura distribuida.

j) Deberá tener la capacidad de desactivarse durante las ventanas de tiempo para mantenimiento, con el fin de no generar notificaciones ni afectar los niveles de servicio durante intervenciones planeadas.

k) Proporcionar mapas jerárquicos de la topología tomando como base el elemento observado y permitir expandirlos para mostrar su interrelación con el resto de los elementos.

l) La solución deberá permitir el análisis en detalle o "drill-down" desde los mapas para llegar a un elemento final determinado, haciendo clicks sucesivos dentro del mapa jerárquico. Todos los mapas deben proveer de un mecanismo de "regreso" a la capa superior de la que se proviene en dicho drill-down.

m) La solución propuesta deberá tener la capacidad de monitorear, filtrar, correlacionar y responder a eventos generados a partir de dispositivos de red, servidores, aplicaciones y equipos de almacenamiento.

n) La solución deberá contar con la capacidad de exportar la información de las alarmas a archivos de bitácora con la finalidad de que puedan ser explotadas.

o) La solución deberá tener la capacidad de generar y enviar alarmas o eventos vía traps SNMP o APIs a otros sistemas.

p) La solución deberá tener la capacidad automática de generar y enviar alarmas o eventos a otros sistemas o dispositivos electrónicos móviles.

q) La solución deberá ser capaz de recibir alertas y/o notificaciones al menos por los siguientes medios o protocolos de administración:

1. Traps de SNMP,
2. Mensajes de Syslog,
3. Lectura de archivos de texto o logs,
4. Correo electrónico,
5. Micro blogs,
6. interfaces de Aplicaciones de Programa (API por sus siglas en inglés).

r) La herramienta deberá tener la capacidad de programar políticas para escalar la atención de eventos que así lo requieran, así como el envío de notificaciones automatizadas vía correo electrónico. La estructura de las notificaciones y la relación de personal del Instituto, así como su frecuencia y escalamientos serán propuestos por el **LICITANTE**.

s) Consulta de información histórica de comportamientos y tendencias durante la vigencia del proyecto.

t) La herramienta deberá entregar un Tablero de Control que permita tener una visión de 360 grados del servicio mostrando las capas que lo componen incluyendo aplicaciones, infraestructura y dispositivos monitoreados.

u) La solución deberá ser capaz de guardar históricos de la visibilidad al menos por 3 meses.

v) La solución deberá contar con umbrales dinámicos determinados por el aprendizaje del comportamiento de los elementos vigilados, así como umbrales estáticos de advertencia y de alerta.

w) La solución deberá ser capaz de entregar distintas vistas de la salud, estado y desempeño de los BCF, BCC y soluciones, de acuerdo a perfiles de usuario. De manera enunciativa más no limitativa, se enlistan las posibles vistas:

a. Operativas. Vistas orientadas al personal que se encarga de vigilar el estado de salud de los BCF, BCC y servicios. Esta vista está destinado a la vigilancia del servicio por el personal del **LICITANTE**.

b. Gobierno y control. Vistas para el personal de operaciones del Instituto a fin de que conozcan el estado del servicio. Esta vista también podrá ser utilizada por el área de

tecnología del Instituto y del **LICITANTE** para la medición interna de los Niveles de Servicio.

c. Ejecutiva. Vista que concentra el estado de todos los servicios del presente anexo técnico, las vistas serán acordadas entre el **LICITANTE** y el Instituto, y será responsabilidad del **LICITANTE** diseñar, implementar y liberar la vista hacia el usuario.

x) El **LICITANTE** deberá contemplar el desarrollo e implementación de las vistas de las aplicaciones y servicios que hoy se encuentran desplegadas en el Centro de Datos actual, debiendo efectuar el análisis, diseño, configuración e implementación, así como el soporte y mantenimiento.

y) El **LICITANTE** deberá de implementar herramientas que permitan medir la Experiencia de Usuario, definiendo en conjunto con el Instituto las aplicaciones y servicios que requieren esta característica de monitoreo, en las mesas de trabajo durante la vida del contrato.

z) Todas las vistas deberán poder hacer consultas históricas y Drill-Down a un nivel suficiente para entender el punto de falla en caso de un evento.

aa) El servicio deberá contemplar el personal para participar activamente en la entrega de evidencias en tiempo real y análisis de los eventos presentados por cada nivel o capa de la solución vigilada, cuando así el Instituto lo requiera.

bb) Dado que las demandas son variables y los servicios y/o BCC pueden cambiar de bloques de construcción que los componen, así como sus relaciones; a fin de lograr la mayor certidumbre en la efectividad de las detecciones positivas o reales de eventos, la vigilancia deberá estar en constante afinación de umbrales y sus correlaciones.

Aspectos Generales de la solución de visibilidad

Monitoreo de infraestructura

Se entenderá como monitoreo la vigilancia de la salud de los BCF de forma independiente. Dichos bloques de construcción deberán estar integrados a la solución de visibilidad como requisito para su liberación y aceptación. El nivel de visibilidad de los bloques de construcción base deberá ser de signos vitales de los componentes que integran el bloque de construcción y sus relaciones o dependencias con las plataformas que lo habilitan.

Análisis de flujos de tráfico

El **LICITANTE** deberá realizar todas las actividades necesarias para que el flujo del tráfico de comunicaciones e se encuentre dentro de los objetivos de nivel de servicio establecidos en la sección de Requerimiento de Niveles de Servicio.

Para tal efecto el **LICITANTE** deberá realizar las siguientes funciones que se enlistan a continuación de manera enunciativa más no limitativa:

a) Análisis de capacidades actuales de los sistemas a ser migrados, así como dimensionamiento y propuesta de infraestructura en Nube privada e híbrida IMSS.

b) Análisis, dimensionamiento y labores de coordinación de la migración de los sistemas de su ubicación original a la ubicación destino.

c) Vigilancia de los flujos de tráfico de la Nube privada e híbrida IMSS.

d) Análisis del flujo de tráfico.

e) Generación de informes y reportes.

f) Generación y ejecución de mejoras para el desempeño y disponibilidad de la Nube.

g) Gestión proactiva y reactiva de incidentes y problemas relacionados con los flujos de tráfico de la Nube privada e híbrida IMSS.

h) Mitigación de los impactos o posibles impactos adversos por vulnerabilidades detectadas.

El **LICITANTE** deberá proporcionar, como parte del servicio, una solución que incluya todo el hardware, software y personal necesarios para la entrega del servicio, la cual deberá ser suministrada, instalada, configurada, implementada, soportada y operada por el **LICITANTE**. Es responsabilidad del **LICITANTE** mantener actualizada las versiones, parches y configuraciones para la correcta operación de la solución.

Las características mínimas que debe cumplir la solución del servicio para el presente anexo técnico se mencionan de manera enunciativa más no limitativa:

a) Sistema de gestión centralizado y que concentre la administración de monitoreo. El monitoreo deberá realizarse por solución tecnológica, los componentes y los riesgos detectados, las áreas de oportunidad detectadas, las acciones de prevención o corrección a realizar a corto plazo y las planeadas a mediano plazo, el plan de trabajo de la implementación de las correcciones propuestas, dependencias y afectaciones a considerar durante la implementación, detalle de los trabajos de la implementación de las acciones de prevención / corrección, el detalle de la implementación, los registros y bitácoras, las consideraciones futuras detectadas durante la implementación y las acciones de supervisión sugeridas con motivo de la implementación de acciones preventivas o correctivas.

b) Portales web con vistas personalizadas por grupo de interés donde se pueda monitorear el tráfico y riesgos según perfil, y que permita crear limitación de opciones del menú de cada perfil.

c) Generación y entrega de reportes de riesgos detectados y mitigaciones 'activas' y detalles de las mitigaciones anteriores. Los formatos de Reporte deberán ser como mínimo XML, PDF, Excel y CSV.

d) Generación y entrega de reportes de tráfico, protocolo, objetos administrados con GeoIP (Regiones basadas en IP) indicando de dónde viene y hacia dónde va el tráfico que se está analizando, de la siguiente forma:

ANEXOS
DIVISIÓN DE CONTRATOS

a. Tráfico por país,

b. Tráfico por región,

c. Tráfico por ciudad

e) Generación y entrega de reportes en tiempo real y en forma programada de eventos que incluyen anomalías clasificadas por niveles de severidad configurables.

f) Despliegue de todas las alertas que contenga al menos la siguiente información: hora de inicio, hora de término y tipo de alerta.

g) Búsqueda de información del tráfico monitoreado.

h) Capacidad de realizar anotaciones y clasificaciones dentro de la alerta.

i) Detección a través del monitoreo de patrones de Ataques de IPv6.

j) Representaciones gráficas de tasa de transferencia de datos, ataques, vulnerabilidades, a través del tiempo para períodos de tiempo variables al menos hasta tres años.

k) Integración con otros sistemas de gestión que el Instituto indique, mediante Interfaces de Aplicaciones de Programa (API), para la gestión de eventos y análisis de flujos de tráfico.

l) Generación de información de DNS (FQDN/RDN más requeridos), HTTP y VOIP (SIP).

m) Conexión transparente a la infraestructura del Instituto, de tal forma que no entorpezca el tráfico normal, o le sume un retardo que pueda afectar la eficiencia de la red ante los servicios sensibles.

n) La solución deberá soportar al menos los siguientes protocolos de gestión:
   a. Secure Web-based GUI.
   b. CLI: Console, Telnet, SSH.
   c. SNMP MIB and MIB II.
   d. RADIUS.
   e. Syslog.

o) Análisis y filtrado dinámicamente de al menos los siguientes ataques:
   a. DNS.
   b. HTTP Get flood.
   c. Conexiones Inactivas.

p) Capacidad de monitoreo de servicios:
   a. Valor agregado en servicios VoIP (SIP), Servicios basados en TCP
   b. Definición de Servicio con base en la dirección IP, Protocolo, Puerto, Firmas digitales (fingerprints).

c. Monitoreo de características de rendimiento como RTT, jitter, pérdida de paquetes e impacto a los servicios
d. Base histórica de servicios específicos de datos como códigos de respuesta en SIP, DNS, HTTP.
e. Reportes de cambios en el servicio como RTT, Throughput, Jitter

q) Detectar a través del análisis de tráfico los elementos necesarios para lograr controlar acciones que influyan en el ancho de banda de la red, eventos tales como Worms, spam y otras aplicaciones residentes en los equipos terminales, que pueden afectar el desempeño de la red o a otros usuarios.

r) La solución deberá identificar patrones de tráfico seleccionados y redireccionarlos en redes BGP hacia un sistema que permita al administrador aplicar filtros de tráfico con base en los criterios que establezca el Instituto.

s) Tipificación y evaluación de los niveles de tráfico en la Nube privada e híbrida IMSS

Mitigación de impacto por detección de ataques

El servicio deberá incluir mecanismos para la mitigación de impactos adversos por detección de ataques o posibles ataques, con las siguientes características:

a) Sistema de mitigación independiente a la infraestructura actual, es decir, que no requiera módulos que se instalen en chasis existentes.

b) Interactuar con la infraestructura del Instituto de tal forma que, una vez que se detecte un ataque, éste pueda ser eliminado del tráfico en curso.

c) Analizar el tráfico y crear dinámicamente los filtros que se adapten constantemente, según las características de la zona que se esté protegiendo y el tipo de ataque detectado con el fin de poder eliminar únicamente el tráfico dañino, sin requerir para operar de modo óptimo, de un monitoreo previo del tráfico por parte del equipo de mitigación.

d) Proveer la opción de Auto Mitigación, donde el sistema hace la detección y la mitigación y que se realice en forma automática, sin intervención humana.

e) Capacidad de despliegue de Mitigaciones en tiempo real:
a. Visibilidad en tiempo real de los eventos de la mitigación
b. Visibilidad de todas las estadísticas de las mitigaciones andando
c. Selección de detalle y configuración de cada contra-medida usando la pizarra de mitigación
d. Captura simple de paquetes de datos "crudos" directamente desde la pizarra de mitigación
e. Análisis de paquetes en tiempo real que permita lo siguiente:
I. Depurar amenazas emergentes en tiempo real antes de aplicar contramedidas.
II. Análisis de protocolos de red

ANEXOS
DIVISIÓN DE CONTRATOS

f) Soporte de las siguientes contramedidas de Mitigación:

a. Global Exception and Black / White List
b. Zombie Removal
c. TCP SYN Authentication
d. HTTP Authentication
e. DNS Authentication (Pasivo y Activo)
f. DNS NXDOMAIN Rate Limit (para ataques de diccionario)
g. TCP Connection Reset
h. Payload Regex Filtering en HTTP
i. Baseline Enforcement
j. Rate Limiting en HTTP Request, HTTP Object, SIP Request
k. Malformed Filtering en HTTP, DNS, SIP.

g) Capacidad de tomar acciones ante diferentes eventos. Al menos debe poder tomar las siguientes acciones:

a. Bloquear el tráfico anómalo sin afectar el paso de tráfico válido.

b. Alertar al operador.

El Instituto será responsable de aportar información necesaria para la Implantación del servicio, así como de dar las facilidades para las pruebas de integración. Lo anterior será propuesto por el **LICITANTE**.

La parametrización de la aplicación deberá trabajar con el enfoque de que, únicamente, lo explícitamente aprobado por el Instituto, es permitido.

Las alternativas de solución que el LICITANTE ofrezca al Instituto deberán tener fundamentos de posicionamiento en el Mercado, y en la evaluación de los costos se debe considerar los de implantación del servicio, así como los costos por los servicios y su operación, mantenimiento y soporte durante la vida del contrato.

Para el suministro de la funcionalidad arriba mencionada, el Instituto proporcionará los accesos y facilidades en los equipos a monitorear de acuerdo a las políticas de seguridad vigentes y a los alcances de los contratos correspondientes.

La solución deberá tener la capacidad de colectar tráfico BGP, SNMP, Netflow, Sflow, Cflow y que a partir de este tráfico pueda identificar patrones maliciosos que potencialmente puedan afectar la disponibilidad de lgos servicios, así como la Implantación de un monitoreo de desempeño transaccional con gran capacidad de almacenamiento, la integración de esta herramienta debe permitir la rápida y eficiente consolidación, análisis, contextualización y alertamiento con fines preventivos y reactivos de eventos que puedan afectar la disponibilidad y el desempeño de las aplicaciones del ambiente de operación de la Nube privada e híbrida IMSS.

En redes BGP, la solución deberá tener la capacidad de identificar patrones de tráfico seleccionados por el administrador y redireccionarlos hacia un sistema, parte de la solución, que permita al administrador aplicar filtros de tráfico con base en su criterio para eficientar, en caso de ser necesario, el uso de ancho de banda.

Visibilidad de servicios digitales y de información

Se entenderá como visibilidad a la vigilancia del estado y desempeño de BCCs, plataformas y servicios en el presente anexo técnico.

El **LICITANTE** llevará a cabo el mapeo y vigilancia de punta a punta, esto es, deberá vigilar el estado y desempeño de cada uno de los componentes de un BCC, plataforma, servicio o solución que esté alojada en la el centro de datos ofertado por el **LICITANTE**, tomando en cuenta la relación y dependencia de sus elementos (red, procesamiento, base de datos, almacenamiento, etcétera), así como el flujo y desempeño aplicativo. Para cada implementación de visibilidad deberá realizarse un diseño específico basado en la arquitectura de la solución.

La implementación de la visibilidad deberá cubrir como mínimo los dominios de Signos Vitales, Aplicación y Experiencia de Usuario de forma integral mediante la correlación de eventos.

El **LICITANTE** deberá entregar de manera mensual la evidencia documental que soporte las acciones referentes a este apartado, específicamente en el documento con evidencia de la herramienta tecnológica para la visibilidad de los servicios.

Para el caso de los requerimientos puntuales sobre el acceso y terminales de visualización que incluye Hardware y Software para la entrega del servicio de monitoreo, el **LICITANTE** entregara de manera formal al Instituto al inicio del contrato, en las fechas acordadas en las mesas de trabajo al inicio del presente contrato.

4.2.1.3.2. Soporte

Será responsabilidad del LICITANTE incluir en el servicio todos los elementos para asegurar la correcta operación, soporte y continuidad de la solución tecnológica para la entrega del servicio:

a) Soporte por parte del fabricante.

b) Actualizaciones de releases, versión y certificados

c) Parches para el producto y alertas para problemas de alto impacto y correctivos de emergencia.

d) Resolución de problemas por parte del fabricante.

e) Soporte de integración de producto y multiplataforma.

f) Acceso a documentos de conocimiento, información sobre compatibilidades

g) Acceso a foros, comunidades, boletines y otras fuentes de información por parte del fabricante.

h) Revisión y optimización de las bases de datos de las herramientas de monitoreo.

Realizar análisis de causa-raíz sobre problemas de desempeño que puedan presentarse sobre las herramientas del presente anexo.

4.2.1.3.3. Proceso de Gestión de Configuraciones

La gestión de la base de datos de configuraciones (CMDB) tiene como principio registrar y mantener actualizada la información concerniente a los elementos de configuración (CI) de la infraestructura operativa que se tienen para proporcionar los servicios del presente anexo técnico. Presentar al Instituto un plan de trabajo para mantener la CMDB Actualizada como parte de las actividades de ejecución del contrato.

La solución deberá proveer un API (Application Programming Interface) o un desarrollo compatible en la funcionalidad para lograr la integración entre herramientas del **LICITANTE** y del instituto. Esta integración debe contemplar el inventario de los componentes tecnológicos de los servicios o aplicaciones que le han sido transferidos al **LICITANTE** para su soporte y operación, por lo que el **LICITANTE** ganador deberá considerar todo lo necesario para llevar a cabo dicha integración, considerando los desarrollos y herramientas necesarios para llevarlo a cabo, sin costo adicional para el Instituto.

El **LICITANTE** deberá designar un **coordinador de configuraciones**, quien deberá tener las siguientes actividades:

- Asegurar la actualización de la CMDB.
- Notificar al instituto los cambios realizados.

El **LICITANTE** deberá entregar de manera mensual el Reporte de Gestión de Configuraciones que soporte las acciones referentes a este apartado.

Aspectos generales del apartado Soluciones Tecnológicas del Centro de Continuidad Operativa

El **LICITANTE** deberá ofertar, detallar, documentar, proporcionar, habilitar, configurar, poner a punto, operar y gestionar la operación e incluir en su propuesta todo lo necesario para dar cumplimiento al rubro de **Soluciones Tecnológicas del Centro de Continuidad Operativa** requerido por el Instituto en el presente anexo técnico, apéndices anexos, términos y condiciones, oferta del licitante y documentación contractual.

4.2.1.4. Contraprestación del servicio

El servicio de **Continuidad a la Operación y Soporte** será devengado mensualmente previa aceptación del servicio por el Grupo de Administración del Contrato.

4.2.2.Consumo de BCFs y BCCs para el Servicio

El servicio **Continuidad a la Operación y Soporte** permitirá el consumo de todos los BCFs y BCCs en modalidad de despliegue "M1: Centro de Datos externo (Centro de Datos Primario)" igualmente se encargará del despliegue de aquellos BCFs y BCCs que correspondan a sus funciones en las modalidades de

0036

despliegue "M3: Extensión de Nube Privada (ENP) en los puntos con mayor demanda transaccional de operación de los servicios del Instituto" y "M5: Instalaciones designadas por el Instituto".

El **LICITANTE** deberá entregar de manera mensual el **Informe de Consumo y Disponibilidad de los BCFs y BCCs** que soporte las acciones referentes a este apartado.

4.2.3. Plataformas para el Servicio de Continuidad a la Operación y Soporte

4.2.3.1. Plataforma de Virtualización en M1 (PVM1)

a) El LICITANTE deberá suministrar una plataforma de virtualización que soporte las diferentes tecnologías de sistema operativo en la modalidad de despliegue M1.

b) Debe incluir todo el software y hardware, así como licencias de software, instalación, configuración, puesta a punto, soporte, operación, administración y todo lo necesario para su correcta implementación.

c) Debe soportar la creación y administración de máquinas virtuales, así como la configuración de toda la solución conforme a lo requerido por el Instituto.

d) El Instituto podrá solicitar durante la vigencia del contrato servicios de virtualización solicitados para las tecnologías que tenga establecidas el Marco Tecnológico de Referencia del Instituto.

Actividades que deberá realizar el **LICITANTE** como parte del servicio de plataforma de virtualización:

a) Instalación, Configuración y administración de la consola de administración para la plataforma de virtualización.

b) Creación de nuevas máquinas virtuales que se necesiten por nuevas necesidades del Instituto.

c) Configurar la solución de virtualización a efecto de proporcionar de manera temporal, dinámica y sin afectar ninguna de las máquinas virtuales involucradas, capacidad extra a una o más máquinas virtuales durante un intervalo de tiempo determinado con el fin de atender procesos que requieran ocasionalmente más recursos de procesamiento y/o memoria.

d) Configurar la solución de virtualización a efecto de permitir mantenimiento a los equipos físicos, dándose de baja de manera automatizada y transparente para el data center virtual, moviendo máquinas virtuales a otros nodos activos.

e) Configurar la solución de virtualización a efecto de mantener un balanceo dinámico de los recursos de hardware asignados a una o más de las máquinas virtuales del Instituto, relocalizando máquinas virtuales en nodos con menor carga de trabajo sin sufrir afectación de ninguna clase en las mismas.

f) Configurar la solución de virtualización a efecto de prevenir interrupciones en el servicio a causa de fallas de hardware, proporcionando un ambiente de alta disponibilidad en hardware que permita localizar de manera automática y sin afectación alguna en los servicios o procesos las máquinas virtuales del Instituto en uno o más nodos activos.

g) Configurar la solución de virtualización para mover máquinas virtuales entre servidores físicos y/o sistemas de almacenamiento tipo SAN/FC, iSCSI y NFS sin la necesidad de apagar las máquinas virtuales,

es decir, debe poder migrar máquinas virtuales entre máquinas físicas en línea y sin interrupción en la disponibilidad de las aplicaciones y servicios que residen sobre las máquinas virtuales.

h) El software de Virtualización debe de tener la capacidad de utilizar switches distribuidos que existan a través de dos o más hosts que pertenezcan a un clúster y a su vez se administren de forma centralizada, además los switches distribuidos deben de cumplir con los siguiente:

a. Soporte de VLANs privadas
b. Soporte de L2 Forwarding
c. Soporte de IEEE 802.1Q VLAN Trunking
d. Soporte de VLAN Segmentation

i) Configurar la solución de virtualización a efecto de realizar la virtualización de equipos físicos o la conversión de máquinas virtuales en formatos de una plataforma de virtualización a otra.

j) Configurar la solución de virtualización a efecto de realizar la instalación y actualización al software de virtualización, empleando la consola central de administración como medio de envío (deployment) de dichas instalaciones y/o actualizaciones sin necesidad de interrumpir los servicios de las máquinas virtuales.

k) Configurar la solución de virtualización a efecto de crear mensualmente, sin caer en interrupciones del servicio, imágenes de máquinas virtuales activas o inactivas a manera de respaldo o con el fin de mantener máquinas virtuales para probar actualizaciones o parches permitiendo analizar el comportamiento del sistema operativo o sus aplicaciones.

4.2.4.Servicios eventuales para la Continuidad a la Operación y Soporte

A lo largo del servicio de **Continuidad a la Operación y Soporte**, se señalan una serie de servicios que pueden ser consumidos de manera eventual. Dichos servicios serán cotizados de manera individual.

4.2.5.Servicios extendidos

Conforme a lo señalado en la sección **Elementos comunes de los Servicios**, los servicios extendidos se derivan del Servicio de Continuidad a la Operación y Soporte, así como lo relacionado a la Plataforma de Virtualización.

El **LICITANTE** deberá entregar de manera mensual la evidencia documental que soporte las acciones referentes a este apartado relativas a: Informe de los servicios extendidos derivados del servicio de Soporte a la Continuidad Operativa e Informe de los servicios extendidos si es el caso derivados de la Plataforma de Virtualización.

4.3 Servicios de Integralidad y Telecomunicaciones

4.3.1 Soporte para la Integralidad

4.3.1.1 Servicio de soporte de Extensión de Nube Privada

El **LICITANTE** ofrece un servicio de mesa de servicio que:

- Coordine las actividades de despliegue
- Atienda las solicitudes de asignación de tickets relacionados a los PANs y ENs de cada Nodo de Extensión de Nube Privada
- Coordinación de actividades de comunicaciones en la zona de atención de cada Nodo de ENP
- Coordinación de actividades de personal en sitio según se especifica para cada Nodo de ENP en la sección Nodo de Extensión de Nube Privada

Igual deberá considerar el servicio de preparación de BCCs para ENs específicos a cada necesidad de los inmuebles en los que se preste el servicio, estos BCCs podrán contener entre otras cosas plantillas de ENs con aplicativos institucionales o específicos del inmueble, aplicaciones de productividad y configuraciones de escritorio. Igualmente deberá observar las políticas institucionales de seguridad y apoyarse para estos fines en los Servicios de Seguridad de Nube IMSS si así fuera necesario.

4.3.2 Consumo de BCFs y BCCs en M3 y M5

El Servicio de Integralidad y Telecomunicaciones podrá consumir BCFs y BCCs que se encuentren disponibles para la modalidad de despliegue de nube "M3: Extensión de Nube Privada (ENP) en los puntos con mayor demanda transaccional de operación de los servicios del Instituto" y "M5: Instalaciones designadas por el Instituto" conforme a lo que se especifica en la sección Elementos comunes de los Servicios, será responsable de validar su consumo y disponibilidad valiéndose de la información del **Servicio de Continuidad y Gestión de la Operación**.

4.3.3 Plataformas de Servicios de Integralidad y Telecomunicaciones

4.3.3.1 Punto Neutro de la Nube Hibrida

El Instituto tiene un modelo de telecomunicaciones para interconectar múltiples proveedores y múltiples tecnologías, formando una red híbrida, que se convierta en el Punto Neutro de comunicaciones. De esta manera las distintas necesidades del IMSS convergen permitiendo el crecimiento de servicios de transmisión de datos sin dependencias de un solo proveedor, con un marco tecnológico de conexión estandarizada, controlada y segura entre redes permitiendo tener una latencia optimizada.

Las características del Punto Neutro son:

- Redundancia: Permite la conexión de varios puntos de acceso a Internet, a la red interna del IMSS, o de proveedores de servicios digitales, de acuerdo a los lineamientos establecidos por el IMSS, habilitando redundancia de acceso; en caso de que un enlace sufra una caída en el servicio. El Punto Neutro tiene la infraestructura necesaria para recibir a los múltiples enlaces provistos por uno o varios Proveedores.
- Confiabilidad: Está ubicado en un centro de datos remoto con un nivel TIER 4, para que permita tener la disponibilidad que este servicio requiere, es redundante en todos sus componentes

- Flexibilidad: Permite conexiones de los diferentes proveedores de enlaces de comunicaciones que requiera el IMSS, mismos que pueden ser sustituidos de acuerdo con las necesidades tecnológicas de la contratante.
- Interconectividad: El Punto Neutro es el centro de conexión de los diferentes LICITANTES, permitiendo el flujo de información de manera controlada entre los diferentes segmentos o redes conectadas, hacia internet, la red MPLS del IMSS, enlaces a otras dependencias de gobierno o privadas, enlaces VPN, así como servicios que puedan utilizar las diferentes aplicaciones del IMSS, como el uso de notificaciones de SMS, Voz, Web y conexiones a servicios digitales terceros M2M o B2B, tales como banca, Administradoras de Fondos para el Retiro, otras instituciones e inclusive aplicaciones comerciales a través del protocolo IP.
- Latencia Optimizada: Al concentrar a las diferentes redes en el Punto Neutro, la latencia que existe en el tráfico de información entre ellas, se vuelve un común denominador permitiendo el control del tráfico de interconexión de manera centralizada en el centro de datos, proporcionando un canal único de alta velocidad.

El punto neutro por su naturaleza imparcial y estándar contempla una capa de red WAN y una de Internet denominada en lo futuro "WAN EDGE" e "INTERNET EDGE", respectivamente. En estas capas es donde se recibirán como su nombre lo indica, los enlaces de Internet y Enlaces o Nubes de Área Amplia de los diferentes Operadores que puedan ofrecer servicios al Instituto.

Las características que cubre este servicio son:

- Interfaces Físicas. Interface RJ45 en cobre a velocidad de 1Gbps y hasta 10Gbpss.
- Interface Ópticas a velocidad Gigabit y 10 Gigabit.
- 5 Clases de Servicio MPLS.
- Infraestructura de Comunicaciones en Alta Disponibilidad tipo "carrier class" dedicada
- Capacidad de contención de fallas, tolerancia a fallas, cambio de conmutación rápida y recuperación sin interrupciones.
- Acceso al centro de datos con doble trayectoria diferente.
- Interconexión de componentes en Malla con enlaces de alta capacidad 40Mbps y 100 Mbps.
- Capacidad de conectar hasta 25 Redes MPLS.
- Capacidad de conectar hasta 30 Enlaces L2L.
- Capacidad para recibir 2500 conexiones de VPN "site to site" en IPSEC de diferentes fabricantes de equipo.
- Capacidad para recibir 500 usuarios de VPN "client to site" en IPSEC de diferentes fabricantes de equipo.
- Monitoreo de Red y Análisis de Tráfico.
- Niveles de Servicio 99.982%.
- Protocolos estándares de la Industria OSPF, BGP4, IPV4, IPV6, MPLS.
- Fácil crecimiento de anchos de Banda y escalabilidad en línea o sin disrupción. .
- Aplicación de QoS y VRFS para la capa de WAN.
- Alta disponibilidad con 3 carriers de internet para garantizar el servicio.
- Capacidad y disponibilidad de interactuar en conjunto con otro **LICITANTE** de servicios para lograr automatizar la redundancia a las comunicaciones del Instituto tanto en la capa de WAN como la de Internet.
- El apego a las políticas de acceso físicas al Punto Neutro, serán las estipuladas por el **LICITANTE** y acordadas con el Instituto.

El Servicio de Punto Neutro provee capacidades seguras de los puntos de interconexión, así como para la conectividad con los distintos tipos de redes, según se defina por los Servicios de Seguridad de la Nube IMSS.

4.3.3.1.1 Servicio de Conectividad del Punto Neutro

El Punto Neutro cuenta con la capacidad de conectividad hacia otras redes o nubes públicas que utiliza el Instituto para dar comunicación a sus inmuebles a nivel nacional, con distintos niveles de criticidad.

La implementación de cada conectividad de una nube privada hacia el Punto Neutro tiene un cargo por implementación realizada y será devengado una vez que haya sido aceptado por el Instituto de acuerdo con los criterios establecidos en el presente Anexo Técnico.

A continuación se definen las distintas conectividades y las características que se cumplen actualmente.

4.3.3.1.1.1 Unidad de Conectividad MPLS (UCMPLS)

Redes MPLS

Son las redes de área amplia privadas para proveer servicios de telecomunicaciones. De acuerdo con las necesidades de conectividad del Instituto, así como con las diferentes nubes, incluyendo los sitios en donde se habilitan las extensiones de nube privada.

Los enlaces son entregados en los distintos centros de datos privados, públicos o híbridos tanto principales como secundarios que determinó el Instituto incluyendo los sitios donde se habilitaron las extensiones de nube privada, en los que se solicitaron para poder transportar los datos hacia el Punto Neutro, el cual es el nodo principal de las redes Punto a Punto y Multipunto de las redes nacionales.

En específico, la red MPLS (Multiprotocol Label Switching por sus siglas en inglés), tiene como objetivo principal, transportar el tráfico entre los diferentes puntos remotos por medio de un etiquetado y "switcheo" de paquetes dentro de un "backbone" del carrier que en su caso, proporcione los servicios, de tal forma que la comunicación es "full mesh". Por lo que se garantiza técnicamente la velocidad y eficiencia de la red para transportar los paquetes de datos, video y voz.

El **LICITANTE** adjudicado brinda enlaces bajo demanda, con la tecnología MPLS (Multi-Protocol Label Switching), que solicitó el Instituto, soportando realizar funciones tales como:

Ingeniería de tráfico o administración y modelado de ancho de banda, que permita asignar prioridades, garantizar ancho de banda específico (por aplicación, protocolo, horario IP, etc.) así como utilizar el ancho de banda de manera dinámica.

Políticas de Enrutamiento (Policy Routing) para direccionar el tráfico según criterios establecidos, como: la dirección origen del paquete, el tipo de tráfico o cualquier otra información contenida en el paquete.

Clase de Servicio (CoS Class of Service), que permita identificar el tráfico de datos, de video y/o de voz.

Calidad de Servicio (QoS Quality of Service), que permita asignar colas de prioridad para garantizar la prioridad de aquellos paquetes sensibles al retardo (video y voz) de los que no lo son.

Mapa de Enrutamiento (Route Map), que permite la discriminación o desvío de tráfico específico, a través de listas de acceso o listas de prefijos.

Restricción de tráfico por Listas de Acceso.

Se cuenta con los medios que permiten atender las solicitudes que formule el Instituto sobre enlaces MPLS, para que estos puedan operar bajo los siguientes tipos y características:

- Activo – Pasivo. En este esquema, un enlace se encuentra funcional (primario) y el otro está disponible (respaldo o secundario) para que en caso de falla del primero, se conmute el tráfico hacia el de respaldo, con un tiempo de afectación mínimo. Se debe incluir además el transporte, la conmutación así como el enrutamiento de paquetes, a conveniencia o solicitud del Instituto.
- Activo – Activo. En este esquema, ambos enlaces están disponibles para el transporte de paquetes, en caso de falla de alguno de los dos el que quede disponible absorbe todo el tráfico, por lo que no existe tiempo de afectación; en estos enlaces se balancea el tráfico. Se incluye además el transporte, la conmutación así como el enrutamiento de paquetes, a conveniencia o solicitud del Instituto.

Las características que cubre este servicio son:

- Incluye VRF (Virtual Routing and Forwarding por sus siglas en inglés)
- Para Interfaces físicas en cobre, estas son 1000BaseTX RJ45 con una velocidad de 1 (un) Gbps.
- Para Interfaces físicas con fibra óptica multimodo BaseSX con velocidad 1 (un) Gbps y 10 (diez) Gbps.
- Incluye Clases de Servicio (CoS) y Calidad de Servicio (QoS).
- Infraestructura de comunicaciones en alta disponibilidad.
- Direccionamiento IP privado con la validación del Instituto.
- Capacidad de conectar una Red de MPLS con un enlace central mínimo de 100 Mbps con incrementales en múltiplos de 10, 20, 100 y 200 Mbps, en el Ancho de Banda, hasta un límite máximo de 10 Gbps.
- Monitoreo de red y análisis de tráfico.
- Protocolos estándares de la Industria, ruteo estático, OSPF, BGP4
- Flexibilidad para crecimiento de anchos de Banda y escalabilidad en línea y sin disrupción.

Cuenta con la capacidad y disponibilidad de la infraestructura que permita recibir enlaces de los diferentes carrier's para soportar la conectividad requerida en el Punto Neutro.

El apego a las políticas de acceso físicas al Punto Neutro, serán las estipuladas por el Prestador del Servicio y aprobadas por el Instituto.

Unidad Incremental de Conectividad MPLS (UCMPLS)

Actualmente contamos con la flexibilidad de incrementar o decrementar el Ancho de Banda a solicitud del Instituto.

Los incrementos de Ancho de Banda se llevarán a cabo en múltiplos de 10, 20, 100 y 200 Mbps hasta un límite máximo de 10 Gbps, considerando que el crecimiento de anchos de banda y escalabilidad se lleve a cabo en línea y sin disrupción.

4.3.3.1.1.2 Unidad de Conectividad Enlaces Dedicados (UCED).

Esta unidad de servicio tiene variantes por lo que su integración se fundamenta en los acuerdos que se establezcan bajo la demanda del Instituto.

Este tipo de Enlace corresponde a un enlace MPLS el cual fue definido previamente en el presente anexo.

4.3.3.1.1.3 Enlaces "LAN to LAN".

Actualmente contamos con servicios de enlace LAN to LAN (L2L) los cuales brindan una extensión del direccionamiento LAN del sitio del Instituto que se trate, hacia el sitio que el Instituto defina. Lo anterior con el fin de mantener el mismo dominio de "broadcast" mediante un enlace Ethernet. Las interfaces pueden ser de fibra óptica o cobre.

Las características que deben cubrir este servicio son:

- Interfaces físicas en cobre (RJ45) u ópticas (Conectores LC-LC) a velocidad al menos de 1 Gbps.
- Interface óptica con fibra Multimodo a velocidad al menos 1 Gbps y hasta 10 Gbps.
- Infraestructura de comunicaciones en alta disponibilidad.
- Direccionamiento IP privado con la validación del Instituto.
- Capacidad de conectar al menos 1 (un) enlace "LAN to LAN" en múltiplos de 10, 20, 100 y 200 Mbps, en el Ancho de Banda hasta un límite máximo de 10 Gbps. Fácil crecimiento de anchos de banda y escalabilidad en línea o sin disrupción.
- Monitoreo de red y análisis de tráfico.
- Infraestructura dedicada.
- El apego a las políticas de acceso físicas al Punto Neutro, serán las estipuladas por el Prestador del Servicio en acuerdo con el Instituto.
- Los enlaces se reciben en una capa extra de seguridad por medio de un clúster de firewalls que permita realizar la separación y protección de datos en la capa perimetral previo al ingreso de tráfico hacia el centro de datos, mediante políticas de "firewall", tomando en cuenta los requerimientos que la División de Seguridad Informática del Instituto determine.

Unidad Incremental de Conectividad Enlaces Dedicados (UCED).

- El Prestador de Servicios deberá contar con la flexibilidad de incrementar o decrementar el Ancho de Banda a solicitud del Instituto.
- Los incrementos de Ancho de Banda se llevarán a cabo en múltiplos de 10, 20, 100 y 200 Mbps hasta un límite máximo de 10 Gbps, considerando que el crecimiento de anchos de banda y escalabilidad se lleve a cabo en línea y sin disrupción.

4.3.3.1.1.4 Unidad de Conectividad segura vía Internet (UCVPNI).

Conexiones a sitios remotos (Site to Site)

Definición: Son las conexiones que se hacen vía internet de forma segura utilizando hardware dedicado como Routers, Firewalls o UTMs en los inmuebles remotos con el fin de encriptar el tráfico de la red local. Para asegurar los datos se utiliza el protocolo IPSEC como protocolo estándar de la industria. Este tipo de enlaces está sujeto al SLA del ISP que da el servicio en el inmueble remoto y no en el Punto Neutro.

Las características que deben cubrir este servicio son:

- Interfaces Físicas RJ45 en cobre a velocidad de 1Gbps y hasta 10Gbps

- Interface óptica con fibra Multimodo o interface de cobre con UTP cat6A a velocidad de Gbps.
- Infraestructura de comunicaciones y seguridad en esquemas single-instance o high avalability
- Capacidad de conectar multiples Puntos a Punto mediante tecnologías seguras y con equipos Routers, Firewalls o UTMS de diferentes marcas. En incrementales bajo demanda con dispositivos de diversas capacidades según el volúmen y requerimiento específico.
- Arquitectura de Red Hub and Spoke
- Monitoreo de red, túneles y análisis de tráfico
- Niveles de servicio 99.982%.
- Infraestructura dedicada en cajas Firewalls en modo "clúster" para los componentes centrales en punto neutro.
- Capacidad de configurar protocolos de ruteo dinámico para lograr redundancia automática de los túneles con algún otro tipo de enlace que llegue en los inmuebles de la contratante.
- Alineación de los servicios con las políticas de seguridad del Instituto.
- El apego a las políticas de acceso físicas al Punto Neutro, serán las estipuladas por el LICITANTE en conjunto con el Instituto.
- El centro de operaciones de red y seguridad del **LICITANTE**, realiza actividades de administración de los sistemas de seguridad, incluyendo el soporte técnico, monitoreo, manejo de incidentes de seguridad y administración de la configuración (altas, bajas y cambios), en un horario de 7 días de la semana x 24 horas al día x 365 días del año.

Unidad de Incremento de Conectividad VPN segura vía Internet (UICVPNI).

- El incremento de este servicio será en bloques de 50 sitios a conectar vía VPN's a Punto Neutro, mediante túneles de IPSec y con equipos firewalls o UTMS de diferentes marcas.

4.3.3.1.1.5 Unidad de Conectividad de Internet. (UCI).

Deberá proveer conectividad hacia los servicios web nacionales y mundiales.

Deberá considerar e incluir todas las medidas de seguridad perimetral así como los componentes necesarios que permitan realizar una navegación Web segura, íntegra, confiable, estable y rápida.

Deberá tener la flexibilidad para soportar crecimiento en Ancho de Banda en múltiplos de 10, 20,100 y 200 Mbps hasta un máximo de 10Gbps.

Dentro de la infraestructura del servicio de Internet se deberán considerar los siguientes elementos:

- Enlaces limpios (Clean Pipes),
- ingeniería de tráfico que contemple la administración y modelado de ancho de banda en el medio de transmisión.

4.3.3.1.1.6 Unidad de Incremento de Conectividad de Internet. (UICI).

- Capacidad de conectar diferentes enlaces de Internet con capacidad de recibir todas las tablas de ruteo en una interface de 1 Gbps con incrementales de 1Gbps y hasta 10 Gbps.
- Los incrementos de los enlaces físicos de Internet tendrán que ser en interfaces de Gbps, óptico o en cobre.
- La configuración inicial de la interfaz física a Gbps será de 100 Mbps.
- Los aumentos de ancho de banda serán de manera lógica con limitación de ancho de banda en múltiplos de 100 Mbps hasta llegar a 10 Gbps.

4.3.3.1.2 Comunicaciones

- **Anchos de banda**

Los servicios actuales atienden las solicitudes del Instituto con respecto a incrementos y/o decrementos en múltiplos de 10, 20, 100 y 200 Mbps en el Ancho de Banda, hasta un límite máximo de 10 Gbps para cualquier tipo de enlace que forme parte de los servicios solicitados en el presente anexo.

Constantemente se brinda el servicio de visibilidad donde se realiza el monitoreo de forma continua del uso de los recursos de red (por ejemplo, anchos de banda, disponibilidad, paquetes perdidos, etc.) para asegurar el nivel de servicio acordado.

El Prestador del Servicio, en conjunto con el IMSS, define las reglas de uso de los recursos y umbrales que servirán como referencia para disparar el crecimiento de las facilidades y capacidades de los enlaces con base a los reportes y notificaciones de capacidad.

En el servicio de visibilidad actual se envían mensajes cortos y/o correo electrónico al IMSS, de forma que se pueda decidir sobre el incremento de capacidad en los sitios en donde se haya excedido los umbrales.

4.3.3.1.2.1 Conectividad

Actualmente suministramos los diferentes componentes habilitadores como son enlaces y redes que permitan transportar a través de ellos de uno a otro u otros sitios paquetes de datos, video y voz, así como también deberá incluir el equipamiento requerido de comunicaciones, seguridad y los insumos

Estamos alineados y apegados a los estándares de comunicaciones y seguridad, así como a las mejores prácticas de la industria que garanticen técnicamente la confidencialidad, disponibilidad e integridad de los datos o información que se trasmitirá a través de los enlaces o redes que proporcione al Instituto.

4.3.3.2 Nodo de Extensión de Nube Privada

El servicio de Extensión de Nube Privada es una modalidad de despliegue de los servicios del presente anexo técnico. Se aprovisiona de manera integral como plataforma para otorgar los servicios digitales avanzados para unidades médico-administrativas. Los servicios facilitan la replicación de servicios e información, y resiliencia a errores que se refiere a la capacidad de permitir a las unidades asignadas al nodo, continuar funcionando con un conjunto específico de sistemas e información de forma local aunque el sitio principal del IMSS u otro punto de gestión central haya quedado sin servicio.

El nodo de Extensión de Nube Privada (ENP) tiene la capacidad de implementar acceso, seguridad, gestión y archivos, usar métodos de sincronización, conectividad o federación para conectarse con el centro de datos principal. Reduce el flujo de tráfico por la WAN entre el nodo de ENP y el centro de datos principal, aumentar la disponibilidad y mejorar la respuesta en sitios de mayor relevancia y demanda de la atención de servicios digitales y de información del Instituto.

El **LICITANTE** proporciona el servicio de ENP bajo demanda en la modalidad de plataforma, proporcionando los siguientes elementos:

- Infraestructura e instalaciones
- Gestión y soporte

- Portal de colaboración
- Puntos de acceso a la nube
- Escritorio en la nube
- Caché de servicios de nube privada

Este conjunto de elementos que conforman la plataforma como servicio ENP, es provista bajo demanda, la demanda inicial aprovisiona el nodo ENP en la ciudad de Guadalajara aprovisionando un centro de datos móvil soportando la operación del Centro Médico Nacional de Occidente.

La infraestructura administrada soporta y concentra la información de toda la plataforma de cómputo de manera eficiente, de manera centralizada respalda la información del grueso de usuarios, se administra y monitorea de manera central con grupos de soporte en sitio para brindar el soporte personalizado a usuarios finales.

4.3.3.2.1 Infraestructura e instalaciones

El **LICITANTE** facilita elementos para implementar en las ubicaciones de los ENP, infraestructura que aloje el resto de los componentes del nodo de forma segura y confiable. Las características mínimas que se cumplen actualmente por el **LICITANTE**, son las que a continuación se describen de manera enunciativa más no limitativa:

- Sistema de control de acceso
- Nivel de disponibilidad mínimo del 99.982%
- Un sistema de redundancia eléctrica para soportar condiciones de fallo en el suministro de energía eléctrica desde la línea principal.
- Aires acondicionados de precisión en configuración N+1, todos con microprocesador inteligente que administra la temperatura y humedad relativa de la sección climatizada,
- Gabinetes de 600mm de ancho, 1000mm de profundidad y 42 RMS para instalar infraestructura de los bloques de construcción.
  - Cada gabinete deberá contar con un sistema de rodamientos y rieles.
  - Cada gabinete deberá contar con dos organizadores flexibles para cables.
  - Dos niveles de bandejas tipo escalerilla instaladas de manera perpendicular sobre la parte superior de los gabinetes. Una bandeja para cableado de datos y otra para cableado de potencia.
    - Un sistema de detección temprana de humo
    - Un sistema de protección contra incendios
    - Un panel de control
    - Estaciones de aborto
    - Al menos 2 sirenas/luces estroboscópicas
    - Recipientes de agente aerosol
    - Un dispositivo de grabación de video vigilancia (CCTV)
    - Al menos cuatro cámaras de alta resolución (2 internas y 2 externas)
    - Paredes internas con tratamiento de aislante térmico y acústico de material poliuretano
    - Iluminación LED.
    - Implementación de protección balística ofertada por el posible LICITANTE.
    - Un centro de conexiones eléctricas y entrada de Fibra Óptica.
    - Sistema de energía ininterrumpible (UPS) redundante.

El servicio está soportado por toda la obra civil, acometidas, permisos, traslados, herramientas, materiales, personal, así como todo lo necesario para la correcta operación. El **LICITANTE** mantiene de manera eficiente

cada nodo instalado dentro de las instalaciones del centro médico nacional de occidente como parte de la continuidad operativa.

El **LICITANTE** gestiona a través del coordinador la continuidad de servicio de cada nodo y es quién debe realizar al menos las siguientes actividades:

- Ser el enlace con el Instituto.
- Elabora y da seguimiento a la operación
- Informar de avances, riesgos y temas por resolver
- Realizar las gestiones que requiera el servicio

El Instituto continúa siendo responsable de las instalaciones donde se resguarda el centro de datos del nodo de extensión de nube privada. Para soportar la conectividad al sitio central se mantiene un enlace operativo de alta capacidad de tal forma que se interconecta a punto neutro con las garantías de alta disponibilidad y ancho de banda para soportar la operación de manera adecuada.

Las soluciones tecnológicas que forman parte integral de la plataforma de Extensión de Nube Privada, son aquellas que se implementen para:

1. La relativa a la administración y operación del nodo de ENP
2. La gestión y soporte
3. Plataforma para permitir el despliegue de puntos de acceso y escritorio en la nube
4. Portal de colaboración
5. Caché de servicios de nube privada

Adicionalmente, en los nodos de ENP fueron aprovisionados como Bloques de Construcción Fundamentales descritos en el apéndice "1.Bloques de Construcción" para lo cual el LICITANTE oferta costos específicos para esta modalidad de despliegue. La red LAN dentro de las instalaciones del nodo, y deberá respetar los estándares de interconexión así como deberá presentar flexibilidad en la integración a tecnología legacy de cualquier marca bajo protocolos estándares.

4.3.3.2.2 Servicio de gestión y soporte a la ENP

El **LICITANTE** proporciona todos los elementos necesarios como herramientas, personal, hardware y software para la gestión de los servicios que se entregan en los nodos de ENP. Del mismo modo, proporciona todo lo necesario para el soporte y operación del nodo de ENP, así como los puntos de acceso a la nube y portal de colaboración.

El soporte se proporciona en sitio para los Puntos de Acceso a la Nube cuando así se requiera para lo cual, el **LICITANTE** mantendrá el modelo de operación actual con los recursos y horarios ya establecidos para los 4 hospitales. Cada ENP es capaz de soportar cuanto menos 400 Puntos de Acceso a la Nube (PAN) y 1,200 Escritorios en la Nube (EN), igualmente deberá prever una capacidad de hasta 1000 PANs y 2000 EN.

A continuación se enlistan las actividades a realizar en sitio por el personal de soporte:

- Plan de mantenimiento a los puntos de acceso y periféricos cada 6 meses
- Revisión de fallas físicas
- Configuración de los puntos de acceso
- Reemplazo de piezas
- Instalación
- Reubicación física

El conjunto de personas asignadas a la gestión y soporte de los nodos de ENP serán distintos a los del Centro de Continuidad Operativa y tienen un cargo mensual por nodo de ENP, mismo que se comenzó a devengar una vez aceptada la implementación del nodo de ENP en cada ubicación.

4.3.3.2.3 Puntos de acceso a la nube

Los Puntos de Acceso a la Nube (PAN) son estaciones de trabajo ligeras que se implementaron bajo demanda y permiten el acceso a los servicios de la Nube IMSS, en especial a los EN, así como a la red del Instituto. Los PAN permiten el acceso a uno o varios usuarios (no simultáneo), por medio de identificación que determine el Instituto, teniendo separación de sus perfiles y sin estar estrechamente dependiente el punto de acceso a la nube con un usuario. Estos puntos de acceso son el medio para acceder a los escritorios en la nube, cualquier escritorio en la nube (EN) puede accederse desde cualquier PAN del nodo de ENP que pertenezca, a menos que el Instituto determine lo contrario por alguna definición de Seguridad Informática o por situaciones operativas.

Si el Instituto lo requiere, un EN es accesible desde otros nodos de ENP previo un proceso de migración del EN según lo oferte el **LICITANTE** del servicio, o resguardarse en la nube indeterminadamente hasta que se requiera su acceso desde un nodo de ENP específico.

Los Puntos de Acceso a la Nube y Escritorio en la Nube fueron implementados por el **LICITANTE** en los inmuebles que se encuentran en la cobertura de las redes locales LAN de aquellos inmuebles y campus del Nodo de ENP. Actualmente la infraestructura correspondiente a dichas redes se encuentra operativa en al menos las ubicaciones señaladas en el Apéndice "2. Ubicaciones Geográficas", por lo que el **LICITANTE** puede hacer uso de las mismas para proveer sus servicios, en estos casos el mantenimiento de las mismas está a cargo del **LICITANTE** durante el periodo de uso de las redes que correspondan a cada uno de los PAN. En caso de ser necesario y que el Instituto lo autorice, se podrán realizar actividades de adecuación conforme al consumo de BCFs ofertados bajo la modalidad de "Integración a la Nube Privada".

Ambos elementos implementan las siguientes capacidades:

- Movilidad intrahospitalaria del personal al no depender de un equipo virtual y no físico
- Mejora de la experiencia del usuario al tener una sola interfaz de usuario para todas las ubicaciones.
- Optimización de costos de licenciamiento y soporte en sitio a través de la consolidación de configuraciones por perfiles bajo esquemas virtuales sobre una sola instancia de EN.
- Administración de equipos centralizada, aunque los PAN se encuentren dispersos físicamente.
- Flexibilidad y escalamiento sencillo y rápido en la integración de equipos, aplicativos y almacenamiento.
- Baja demanda de espacio físico, consumos de energía y generación de calor.

La continuidad operativa permitirá brindar servicio a 1306 PANes instaladas en CMNO las cuales brindan servicio a escritorios virtuales para soportar más de 2000 usuarios en la operación continua.

Las implementaciones posteriores a este plan se realizarán por requerimiento y el tiempo de entrega del servicio será determinado y acordado por ambas partes dentro de la respuesta del requerimiento inicial. Estos tiempos serán adicionales a cualquier trabajo requerido para acondicionar la red LAN.

Los tiempos del plan de implementación de cambios a la red LAN, serán sumados al plan de implementación de los puntos de acceso a la nube y al plan de implementación de escritorios en la nube, según aplique el caso, para efectos de niveles de servicio de implementación.

La implementación del punto de acceso a la nube será devengado por evento por cada implementación por lo que el posible **LICITANTE** deberá presentar una propuesta de precio para este servicio. El soporte posterior a la implementación será devengado con el servicio de Gestión y soporte del nodo de ENP.

4.3.3.2.4 Escritorio en la nube

El **LICITANTE** cuenta con servicios administrados que implementen escritorios de trabajo virtuales para clientes finales.

El escritorio cuenta con las siguientes funcionalidades como parte integral del servicio:

- Escritorio de trabajo. Construcción del escritorio que incluye los Bloques de Construcción Fundamental que el Instituto determine en forma de Bloque de Construcción Común.
- Aprovisionamiento y bóveda de identidades. Funcionalidad de sincronización de identidades desde distintas fuentes y la generación del repositorio de identidades. Con esta funcionalidad el usuario consumirá su propia identidad en los sistemas asociados y usará el portal de colaboración del NEP para que restablezca su contraseña o solicitar nuevos permisos en los aplicativos.
- Control de acceso. Funcionalidad para controlar las identidades, proveer autenticación, autorización, y proveer un marco de trabajo para autenticación.
- Correlación de eventos y sistemas de seguridad. Funcionalidad que detecta e integra todos los eventos de autenticaciones, errores, eventos de seguridad, etc. Habilita auditoría de dichos eventos, así como la correlación y remediación de ataques informáticos a nivel del nodo de ENP.
- Gestión de equipo de cómputo. Funcionalidad de gestión de equipo de cómputo ya sea de escritorios virtuales, "zero clients" o equipos de escritorio. Este servicio facilitará la configuración, soporte técnico, gestión de seguridad e inventario de hardware y software; todo esto con el fin de tener mejor control sobre todos los activos que son parte del nodo NEP. Cada usuario podrá tener asignada distinta configuración, aplicaciones y otras reglas dependiendo de su función y perfil que se encuentra definido en la solución de gestión de identidades. Toda la configuración se aplica dinámicamente dependiendo del usuario que realice el acceso al PAN o EN. Todas las validaciones y autenticaciones se podrán hacer de forma local o verificar contra los servicios centrales.
- Sincronización y acceso a archivos. Funcionalidad para sincronizar archivos desde cualquier dispositivo que use el usuario hacia repositorios locales o hacia repositorios remotos en otros nodos NEP o en el centro de datos principal. Además de lo anterior, los usuarios pueden acceder a sus archivos personales o de carpetas compartidas desde cualquier dispositivos, ya sea virtual o de escritorio.
- Gestión de impresión. Funcionalidad para conectar cualquier dispositivo de cualquier sistema operativo hacia cualquier impresora, sin importar marca, conectada a la red.

- Gestión de archivos y carpetas compartidas. Funcionalidad para administración de carpetas compartidas y de gestión de los servidores de archivo. Debe detectar cualquier cambio o evento en el directorio institucional y lanzar tareas de creación, movimiento, borrado, cuarentena o aplicar permisos a archivos o carpetas; así como archivos con extensiones no deseadas y dejarlos en cuarentena de forma automática. Deberá poder crear espacios de almacenamiento de forma automática.
- Autenticación para escritorios de nube. Funcionalidad para que un usuario pueda acceder a múltiples sistemas o aplicaciones a través de las credenciales de autenticación por medio que el Instituto incorporó (AD).

La implementación de cada escritorio en la nube con las características antes descritas, será devengado por evento por cada implementación por lo que el posible **LICITANTE** deberá presentar una propuesta de precio para este servicio. El soporte posterior a la implementación será devengado con el Servicio de Gestión y Soporte del NEP que abarca lo definido en secciones técnicas como plataforma de nodo de extensión de nube privada.

Las implementaciones posteriores a este plan se realizarán por requerimiento y se acordará el tiempo de atención con la respuesta formal a la solicitud inicial por medio de la herramienta de gestión de servicios del **LICITANTE**.

Por cada escritorio en la nube se entregará una identidad asignada a un usuario específico.

En caso de que se requieran identidades que no estén asociadas a un EN ni a los PAN, éstas tendrán un costo adicional por implementación, por lo que el **LICITANTE** deberá presentar la propuesta de precio para este servicio de "Usuario de Acceso a la Nube Privada" (UANP), y deberá garantizar la capacidad de integración de dispositivos diferentes a PAN usando dicha identidad

4.3.3.2.5 Caché de servicios de la Nube Privada

El **LICITANTE** deberá implementar en cada nodo de Extensión de Nube Privada, un caché de servicios de la Nube IMSS que reduzca el consumo de ancho de banda WAN, carga de los servicios alojados en el centro de datos primario, mejorar el tiempo de respuesta de las soluciones comparado con el tiempo de respuesta obtenido desde el centro de datos primario, y habilitar la disponibilidad de operación fuera de línea para los servicios y soluciones del Instituto que incorporen esa característica.

El caché de servicios de la Nube Privada formará parte de la plataforma como servicio Extensión de Nube Privada en cada nodos implementado e integrará funcionalidad de los componentes de la Nube IMSS, los cuales se describen a continuación de manera referencial:

- Notaría
- Gestor de flujo

La integración a este caché de soluciones, servicios o componentes deberán contar con la aprobación del Grupo de Gobierno del Contrato y el Área de Arquitectura del Instituto.

Cada integración será devengada por evento, previa aprobación por el Instituto, por lo que el posible **LICITANTE** deberá hacer una propuesta para este servicio. Para cada integración el **LICITANTE** deberá presentar un plan de trabajo que deberá ser aprobado por el Instituto.

0043

4.3.3.2.6 Funcionalidades generales del servicio

El **LICITANTE** proporciona una política de uso aceptable acordada con el Instituto, que prohíbe el uso de sus servicios para distribuir o almacenar material que sea inapropiado (incluyendo juegos de apuesta en línea), o material que sea ilegal, difamatorio, calumnioso, indecente, obsceno, pornográfico, no permitiendo los juegos de apuesta.

Se cuenta con una arquitectura distribuida que resida en múltiples redes dentro de diversos proveedores de servicio, asegurando con ello que no exista un punto único de fallo.

4.3.3.2.7 Gestión y control de la plataforma

EL **LICITANTE** proporciona un portal web seguro unificado para los productos y servicios que se solicitan dentro del servicio de publicación y contenido. Se cuentan con las siguientes herramientas, reportes, alertas, consola de administración y transferencia de conocimientos:

- El instituto proporciona los controles de accesos necesarios a la plataforma.
- Se proporciona al Instituto la visibilidad y el control de la infraestructura y los servicios propuestos en el presente Anexo técnico, como el estado de funcionamiento en todo momento e históricos diario, semanal, mensual; se logran ver los reportes hasta 3 meses atrás a la fecha de consulta.
- Se proporcionan alertas que informan directamente al Instituto cuando los umbrales definidos se han rebasado, lo que indica que el rendimiento y la experiencia del usuario se han degradado.
- Se provee monitoreo en tiempo real y con la capacidades de generar reportes históricos que ayudan en la evaluación y el mantenimiento de la eficacia de los portales y con su rendimiento, así como con el análisis de los patrones del tráfico de entrega tanto del lado de la infraestructura del Instituto como de la red o plataforma propuesta.
- Proveerá de una vista unificada de la solución incluyendo los tiempos promedio de respuesta y disponibilidad por locación, análisis de error con la capacidad de profundizar por cada página, por objetos en cada página, por códigos de respuesta http, tamaño y suma por cada ítem, dirección de IP del visitante.

4.3.4 Servicios eventuales

A lo largo del **Servicio de Integralidad y Telecomunicaciones**, se señalan una serie de servicios que pueden ser consumidos de manera eventual. Dichos servicios serán cotizados de manera individual según se señala en la sección Catálogo de Servicios.

4.3.5 Servicios extendidos

Conforme a lo señalado en la sección **Elementos Comunes de los Servicios**, los servicios extendidos se derivan del **Servicio de Integralidad y Telecomunicaciones**, del Punto Neutro de la Nube Hibrida y del Nodo de Extensión de Nube Privada en Modalidad Grande.

4.4 Servicio de Operación y Calidad de la Seguridad Informática Perimetral

4.4.1 *Soporte para la Calidad de la Seguridad de la Nube IMSS*

4.4.1.1 Diseño de Arquitectura de seguridad

Con la finalidad de obtener los mejores servicios de seguridad de la información, el área independiente de punto de control de calidad, deberá valorar y en caso necesario actualizar el diseño de la arquitectura del servicio de seguridad, considerando los elementos necesarios para proporcionar la confidencialidad, integridad y disponibilidad de los activos de tecnologías de información y comunicaciones del Instituto.

Esta estrategia permitirá consolidar la integración de servicios, funciones, sistemas e infraestructura tecnológica en busca de mayor eficiencia, productividad y economías de escala.

En lo referente a la administración y control de la seguridad informática, se requiere el diseño de una arquitectura tecnológica integral que tenga por objetivo proveer servicios informáticos e infraestructura tecnológica que operen con altos niveles de disponibilidad y eficiencia, bajo las mejores prácticas de gestión para las Tecnologías de la Información y Comunicaciones.

Esta arquitectura tecnológica integral se conforma por 8 arquitecturas específicas y un centro de operación de la seguridad, que estructuran y dan orden a los diferentes elementos tecnológicos de forma congruente y consistente, para que "el Instituto" obtenga el mayor beneficio en términos de seguridad de la información en el uso de la tecnología.

Estas arquitecturas específicas son:

- Arquitectura de Firewall
- IPS
- DDoS
- Redes Privadas Virtuales
- UTM's
- Filtrado de contenido web
- Antispam
- Antimalware
- Web Access Firewall
- Centro de Operación de la Seguridad

Lo anterior permitirá contar con aplicaciones y sistemas de información segura por diseño y construcción, protegidos y monitoreados en producción. Identificando oportunamente el manejo de las vulnerabilidades, riesgos y amenazas en la infraestructura tecnológica y sus servicios. Proporcionando la administración y soporte con personal informático calificado con sólidos conocimientos y habilidades en el manejo de seguridad de la información.

4.4.1.2 Pruebas y Validación

El LICITANTE del servicio deberá integrar un área independiente a la que instala y opera los servicios de seguridad, cuya función será la de ser un punto de control de calidad de los servicios cuyo objetivo será

validar que los mismos que vayan a entregar o ser entregados cumplan con los requerimientos y niveles de servicio solicitados por el Instituto.

El Instituto a través del área independiente del punto de control, solicitará la realización de pruebas a las diferentes arquitecturas del servicio de seguridad; lo anterior a fin de revisar que las diferentes arquitecturas tecnológicas de los servicios de seguridad operen con los niveles de disponibilidad y eficiencia, bajo las mejores prácticas de gestión para las Tecnologías de la Información y Comunicaciones.

El LICITANTE independiente del punto de control, podrá llevar a cabo verificaciones presenciales o remotas de los servicios ofrecidos a fin de dar certeza de que estos mismos se encuentran establecidos bajo las condiciones del presente contrato.

4.4.1.3 Análisis de Vulnerabilidades

Descripción del servicio:

El Instituto requiere de un servicio que permite ejecutar análisis técnicos especializados sobre los activos de infraestructura de procesamiento y redes que permitan identificar vulnerabilidades nuevas o conocidas.

Detalles del Servicio:

El LICITANTE del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Capacidad para integrarse al menos dos herramientas que permitan complementar los análisis de vulnerabilidad ejecutados.
- Capacidad para identificar los servicios a analizar, incluyendo el número de equipos involucrados y la versión de las plataformas de los sistemas.
- Identificación de vulnerabilidades documentadas en organismos internacionales como el CVE (Common Vulnerability Exposures).
- Identificación de configuraciones por omisión.
- Capacidad para determinar el grado de vulnerabilidad ante técnicas de ataque como:
  - SQL injection
  - Cross Site Scripting
  - Cross Site Request Forgery
  - Sensitive Data Exposure
  - Security Misconfiguration
  - Broken Authentication and Session Management
- Capacidad para elaborar un reporte técnico y/o ejecutivo donde se describa un riesgo asociado a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP llamada "OWASP risk rating Methodology", detallando recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.
- Capacidad para integrar un proceso/procedimiento de implementación de las medidas de remediación y recomendaciones realizadas, así como el integrar soporte técnico en la solución de los problemas presentados.
- Se dispondrá de un número ilimitado de eventos para realizar procesos de análisis de vulnerabilidades bajo demanda y conforme las necesidades operativas.

4.4.1.4 Pruebas de Penetración

Descripción del servicio:

El Instituto requiere de un servicio que permita realizar una serie de pruebas de penetración sobre la infraestructura del Instituto con el fin de buscar huecos o fallas en la seguridad establecida. Todas las pruebas deberán ser realizadas con herramientas e ingenieros especializados.

Detalles del Servicio:

El LICITANTE del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Identificación los servicios o activos de información que sea analizarán, incluyendo el número de equipos involucrados, y la versión de las plataformas de los sistemas analizados.
- Identificación de vulnerabilidades y malas configuraciones.
- Explotación de acceso a los sistemas mediante el aprovechamiento de los huecos de seguridad detectados y/o vulnerabilidades detectadas.
- Evaluación de vulnerabilidades de al menos los siguientes rubros:
  - Autenticación y Autorización
    - Intentos ilimitados de inicio de sesión
    - Insuficiente autenticación
    - Insuficiente autorización
  - Gestión de sesión
    - Predicción de sesión
    - Secuestro de sesión
    - Reproducir sesión
    - Expiración de sesión insuficiente
  - Inyección de código
    - Inyección comando de SO
    - Inyección SQL
    - Cross-site Scripting
    - Inyección LDAP
    - Inyección HTML
    - Parameters Tampering
    - Cookie Poisoning
    - Hidden Field Manipulation
  - Criptografía
    - Fortaleza del algoritmo
    - Gestión de llaves
  - Ataques Lógicos
    - Abuso de funcionalidades
    - Input Field Validation Checking
  - Protección de Datos
    - Transporte
    - Almacenamiento
  - Divulgación de Información
    - Indexado de directorio
    - Path Traversal
    - Manejo inseguro de errores
    - Comentarios HTML

4.4.1.5 Análisis Forenses

Descripción del servicio:

El Instituto requiere de un servicios de análisis de incidentes de seguridad para determinar y documentar en qué consistió a través de la integración de registros o bitácoras que permitan obtener indicios de eventos y su relación en el tiempo y que permitan identificar cuándo ocurrió, qué infraestructura, servicios tecnológicos o sistema de información fueron comprometidos, como fue realizado y quien estuvo relacionado con el incidente y el impacto del evento.

Detalles del Servicio:

El LICITANTE del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Apoyar en la definición del objetivo parámetros y cuestionario que resulten de interés para la investigación solicitada.
- Dar continuidad y seguimiento a los casos solicitados en un tablero de control, así como, el registro de los indicadores correspondientes.
- Preservar la integridad de la información recibida durante la ejecución del proceso de análisis forense.
- Participar en entrevistas y con los principales involucrados con la finalidad de obtener el contexto necesario en las investigaciones digitales realizadas.
- Obtener información de fuentes públicas en la red en caso de que estas pudieran llegar a ser relevantes para la investigación realizada.
- Realizar la evaluación de información en los puestos de servicio para la identificación de malware.
- Realizar un proceso de recuperación de información que haya sido borrada previamente.
- Proporcionar una herramienta colaborativa que facilite la visualización de hallazgos a los usuarios finales, así como generar reporte de hallazgos en caso de ser requerido

4.4.1.6 Borrado Seguro de Datos

Descripción del servicio:

Realizar el borrado seguro de información en servidores, equipos de centros de datos, discos duros externos y otras unidades de almacenamiento, que el Instituto solicite mediante una solución de borrado seguro que imposibilite, ante cualquier intento o medio, la recuperación de la información borrada, que permita la generación de un certificado que respalde la ejecución de borrado y que sea totalmente automatizada y gestionada centralmente.

Detalles del Servicio:

El LICITANTE del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Debe permitir realizar borrados completos en servidores derivados de sustitución de equipos, migraciones tecnológicas o retiro por finalización del contrato.
- Debe asegurar que los datos no puedan ser recuperados, basándose en al menos los siguientes estándares internacionales
  - HMG Infosec Standard 5 (baseline and enhanced),
  - opnavinst 5239.1ª
  - Extended NIST 800-88
  - DoD 5220.22-M
- Borrado de Discos duros IDE/ATA, SCSI, SAS, USB, SATA, Fiber Channel y FireWire de cualquier tamaño.
- Debe brindar la destrucción local y/o remota en múltiples dispositivos de almacenamiento
- Debe posibilitar el desmontaje RAID (SCSI)

- Debe permitir el borrado y detección de zonas bloqueadas / ocultas (DCO, HPA)
- Deberá generar certificados de borrado infalsificables que ofrezcan protección ante cualquier instancia legal, en donde se incluya el resultado del proceso de borrado, fecha, hora, los datos del equipo, el detalle del HD borrado.
- Deberá emitir una firma electrónica para la autenticación de la integridad del reporte de Sanitización emitido por el software de borrado.
- La solución debe poder ejecutarse sin importar de qué sistema operativo se trate.
- El reporte que generé la solución deberá poder ser exportado a un medio de almacenamiento como USB o disco duro.

4.4.1.7 Análisis de Riesgos de Seguridad de la Información

Descripción del servicio:

Identificar, evaluar y manejar los riesgos de la seguridad de la información, utilizando técnicas estadísticas, información histórica, fuentes de información especializada y otras que permitan, determinar la exposición a diferentes escenarios de riesgo, probabilidad e impacto, así como las recomendaciones y líneas de acción, que permitan alcanzar un nivel de seguridad aceptable a un costo razonable enfocado al catálogo de infraestructuras críticas del Instituto.

Detalles del Servicio:

El LICITANTE del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Contexto
  - Recopilar información sobre las operaciones del Instituto, las relaciones entre los procesos de negocio, procesos y recursos de tecnología, las dependencias entre estos, tomando en cuenta:
    - Consideraciones generales del Instituto
    - Definición de criterios básicos para la ejecución del análisis
    - Definición del alcance del análisis
    - Definición del equipo de trabajo del LICITANTE y del Instituto que participará en la ejecución del análisis.
- Valoración de riesgos
  - Utilizar la metodología basada en el proceso ASI del MAAGTICSI para la gestión de riesgos de seguridad. La metodología contendrá:
    - Identificación activos, considerando como activos a los procesos, actividades, información, infraestructura, y gente.
    - Identificación de vulnerabilidades.
    - Identificación de amenazas.
    - Escenarios de riesgo.
    - Priorización del riesgo.
- Tratamiento de los riesgos
  - Criterios para la atención del riesgo identificando y analizando varias opciones de tratamiento de las cuales se elegirá la que mejor balance costo-beneficio genere, considerando el resultado obtenido:
    - Evitar.
    - Mitigar.
    - Transferir.
    - Aceptar.
- Seguimiento y mitigación de riesgos
  - Deberá dar seguimiento a los planes de tratamiento de riesgos conforme lo siguiente:

- La generación de los planes de mitigación de riesgos
- Identificación de los responsables de cada plan.
- Acompañamiento en la implementación de controles normativos.

4.4.1.8 Sistema de Gestión de Seguridad de la Información (SGSI)

Descripción del servicio:

Apoyar al Instituto en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado al MAAGTICSI y basado en el estándar ISO 27001, que permita emitir directivas en materia de seguridad de la información a las áreas de TI y a los terceros que soportan la operación de TI.

Detalles del Servicio:

El LICITANTE del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Planear
  - Capacitación inicial – Curso "Inducción a la norma 27001:2013. Curso introductorio que permite al participante:

Conocer la estructura de la norma ISO/IEC 27001:2013

Interpretar los requisitos solicitados para el cumplimiento de la norma

Conocer las etapas para la implementación de un SGSI

Generación de directivas de seguridad. Manual de políticas de seguridad de la información:

- Basadas en los dominios que establece la norma ISO 27001.
- Alineadas a los procesos de seguridad ASI y OPEC del MAAGTIC SI.
- Enfocadas a las áreas de TI y a los terceros que proveen servicios de TI al Instituto, considerando como alcance el catálogo de infraestructuras críticas del Instituto.

Identificación y valuación de activos (relacionado al catálogo de infraestructuras críticas) del proceso involucrado en el Sistema de Gestión de Seguridad de la Información. La metodología contempla los siguientes puntos:

- Identificación de los activos del proceso.
- Valoración de los activos del proceso.
- Identificación de requerimientos de seguridad.
- Identificación de los controles de seguridad existentes.

Generación de la Declaración de Aplicabilidad. (SoA: Statement of Applicability). La metodología contempla los siguientes puntos:

- Identificación y aplicabilidad de los requerimientos internos y externos:
- Selección de los objetivos de control y controles para el tratamiento de los riesgos
- Verificación de requerimientos contractuales y legales
- Identificación de los requerimientos internos y externos
- Validación de aplicabilidad de los requerimientos

- Formato para la Autorización para implantar y operar el Sistema de Gestión de Seguridad de la Información
- Preparación de la Declaración de Aplicabilidad
- Documentar los objetivos de control y los controles elegidos y la justificación de su elección
- Documentar los controles actualmente implementados
- Documentar la exclusión de controles y la justificación de su exclusión
- Implementar y Operar el Sistema de Gestión de Seguridad de la Información

Análisis de Riesgos de Seguridad de la Información

- Realización del análisis de riesgo con base en lo definido en el servicio de gestión de riesgos de seguridad.
  - Generación del plan de tratamiento de riesgos. La metodología contempla los siguientes puntos:
- Identificación de las acciones a realizar por parte de la organización y su administración
- Identificación de los recursos necesarios y prioridades
- Identificación de las responsabilidades para administrar los riesgos de seguridad de la información

Aplicación del plan de tratamiento de riesgos. La metodología contempla los siguientes puntos:

- Asignación de los roles y responsabilidades en la implantación de los controles relativos a personas, procesos y tecnología involucrados en la mitigación de los riesgos.
  - Actualización de documentación. Alineada a los requisitos establecidos en el proceso ASI y OPEC de MAAGTIC SI.
- Afinación de políticas y procedimientos de seguridad existentes
- Definición del proceso de reporte y atención de incidentes de seguridad (ERISC)
  - Propuestas de implementación de los controles seleccionados: La metodología contempla los siguientes puntos:
- Control de accesos
- Monitoreo de cuentas
- Definición del proceso de Continuidad del negocio
- Implantación de los Roles y responsabilidades definidas para el Sistema de Gestión de Seguridad de la Información
- Controles de seguridad en la infraestructura tecnológica de acuerdo a lo definido en el alcance.
  - Administración del cambio cultural. La metodología contempla los siguientes puntos:
- Desarrollo de un Programa de concientización con usuarios y operadores del Sistema de Gestión de Seguridad de la Información
- Determinación de las necesidades de capacitación para el personal que administra el Sistema de Gestión de Seguridad de la Información
- Apoyo en la capacitación relativa a temas de seguridad de la información.
  - Manual de Gestión de Seguridad de la Información. Se documentará un manual que contiene las referencias de la documentación generada en esta fase para dar trazabilidad al de las cláusulas de la norma
- Monitorear y Revisar el Sistema de Gestión de Seguridad de la Información
  - Revisiones gerenciales. La metodología contempla los siguientes puntos:
- Los dueños del proceso deberán hacer una revisión al Sistema de Gestión de Seguridad de la Información a fin de verificar que los objetivos del Sistema de Gestión de Seguridad de la Información están alineados a los objetivos de negocio en materia de seguridad de la información y que garantizan el adecuado manejo de los riesgos existentes.
- El LICITANTE generará el procedimiento de revisiones gerenciales.
- El LICITANTE propondrá los formatos requeridos para llevar a cabo las revisiones.
  - Auditorías internas. La metodología contempla lo siguiente:

- Apoyo en la generación del plan de auditorías internas a las áreas de TI y a los terceros que proveen servicios de TI al Instituto.
- Definición de los formatos requeridos para llevar a cabo las auditorías
- Aplicación de una auditoría interna al Sistema de Gestión de Seguridad de la Información para verificar el cumplimiento con el estándar ISO/IEC 27001:2013 y a los procesos de seguridad ASI y OPEC del MAAGTICSI
  - Mantener y Mejorar el Sistema de Gestión de Seguridad de la Información
- Implementación de mejoras. Contempla los siguientes puntos:
  - Priorización de las acciones correctivas y no conformidades identificadas en las revisiones gerenciales, revisiones independientes, auditorías internas y revisiones técnicas
  - Identificación de los responsables de llevar a cabo las mejoras por parte de la organización.
  - El Instituto definirá las fechas compromiso para la terminación de las mejoras, únicamente para seguimiento interno.
- Tomar acciones correctivas y en las no conformidades. Contempla los siguientes puntos:
  - Apoyo en la definición del procedimiento para realizar acciones correctivas y no conformidades derivadas de las auditorías.
  - Definición del formato para llenado de acciones correctivas y no conformidades.
  - Coordinación de la ejecución de las acciones correctivas ya definidas y en su caso las no conformidades que se identifiquen.
- Comunicar los resultados de las acciones tomadas. Contempla el siguiente punto:
  - Apoyo en la programación de reuniones de seguimiento al Sistema de Gestión de Seguridad de la Información para dar a conocer el alcance de las acciones correctivas y no conformidades realizadas y verificar su apego a los requerimientos de los dueños de la información y a los involucrados en los procesos del Instituto.

4.4.1.9 Servicio de Seguridad Perimetral para Enlaces de Banda Ancha.

El Instituto requiere un servicio que permita proporcionar la infraestructura que brinde seguridad perimetral para enlaces de banda ancha, a través de los cuales se establece la transferencia de información entre diferentes unidades médicas y administrativas del IMSS.

El servicio de seguridad perimetral para enlaces de banda ancha se requiere en dos modalidades:

- Sitios con un ancho de banda mayor a 100 Mbps y hasta 1 Gbps
- Sitios con un ancho de banda de hasta 100 Mbps.

Las características principales que debe reunir el servicio para Sitios con un ancho de banda mayor a 100 Mbps y hasta 1 Gbps:

- Deberá contar al menos con un rendimiento de 8 Gbps, en su funcionalidad de firewall.
- Deberá tener al menos un rendimiento 1.2 Gbps en su funcionalidad de IPS
- Mínimo deberá contar con 12 puertos 100/1000 de cobre RJ45
- Mínimo deberá contar con 4 puertos de 1 Gbps de fibra
- Mínimo deberá contar con 2 puertos de 10 Gbps de fibra
- Deberá ser un dispositivo de nivel empresarial

- Deberá ser un dispositivo multifuncional, es decir integrar las funcionalidades descritas a continuación, en un solo dispositivo dedicado:
  - Firewall
  - Detección y prevención de intrusos (IPS)
  - Filtrado de contenido de la WEB
  - Detección y control de virus
  - Detección y control de amenazas y programas maliciosos
  - Protección para correo electrónico
  - Detección y control de correo no deseado
- Deberá contar con una consola de administración integrada accesible vía remota y a través de interfaz RJ45
- Deberá contar con doble fuente de poder que pueda ser sustituida en caliente sin afectar al dispositivo y al servicio que presta
- Deberá garantizar técnicamente la seguridad de datos, en situaciones como accesos remotos y comunicaciones de sitio a sitio
- Deberá ser compatible con direccionamiento IPv4 e IPv6
- Deberá contar con la capacidad de manejo de al menos 1024 Vlans.
- Deberá poder operar de manera transparente como un dispositivo Capa 2 y como un dispositivo de ruteo en Capa 3.
- Deberá operar en alta disponibilidad tomando en cuenta los siguientes esquemas.
  - Modo ruteo en capa 3 Activo-Activo
  - Modo ruteo en capa 3 Activo-Pasivo
  - Modo balanceo de carga y conmutación por error.
  - Modo VRRP
- Deberá incluir la capacidad de generar al menos 15,000 túneles VPN a través del protocolo IPSec.
- Deberá poder aplicar QoS (Quality of Service) para priorizar tráfico de Datos, Voz y Video
- Deberá poder crear políticas granulares es decir:
  - Para usuarios
  - Para grupos

Además deberá identificar, permitir, bloquear o limitar el uso de aplicaciones independientemente del puerto, protocolo o técnica evasiva.

- Deberá permitir el escaneo de aplicaciones tales como mensajería instantánea, redes sociales, streaming de video, Voz sobre IP, juegos entre otras.
- Deberá poder realizar autenticación de usuarios a través de Directorio Activo (LDAP), Portal Cautivo, Kerberos, Radius, Tacacs.
- Deberá contar con la administración centralizada de acceso a usuarios, a los recursos del Instituto y aplicaciones en Internet
- Deberá permitir la conexión a las aplicaciones del Instituto a través de dispositivos móviles (Tablet's, SmartPhone's)

Las características principales que debe reunir el servicio para Sitios con un ancho de banda de hasta 100 Mbps:

- Deberá contar al menos con un rendimiento de 3 Gbps, en su funcionalidad de firewall.
- Deberá tener al menos un rendimiento 600 Mbps en su funcionalidad de IPS
- Mínimo deberá contar con 8 puertos 100/1000 de cobre RJ45
- Mínimo deberá contar con 4 puertos de 1 Gbps de fibra
- Deberá ser un dispositivo de nivel empresarial

- Deberá ser un dispositivo multifuncional, es decir integrar las funcionalidades descritas a continuación, en un solo dispositivo dedicado:
  - Firewall
  - Detección y prevención de intrusos (IPS)
  - Filtrado de contenido de la WEB
  - Detección y control de virus
  - Detección y control de amenazas y programas maliciosos
  - Protección para correo electrónico
  - Detección y control de correo no deseado
- Deberá contar con una consola de administración integrada accesible vía remota y a través de interfaz RJ45
- Deberá garantizar técnicamente la seguridad de datos, en situaciones como accesos remotos y comunicaciones de sitio a sitio
- Deberá ser compatible con direccionamiento IPv4 e IPv6
- Deberá contar con la capacidad de manejo de al menos 512 Vlans.
- Deberá poder operar de manera transparente como un dispositivo Capa 2 y como un dispositivo de ruteo en Capa 3.
- Deberá operar en alta disponibilidad tomando en cuenta los siguientes esquemas.
  - Modo ruteo en capa 3 Activo-Activo
  - Modo ruteo en capa 3 Activo-Pasivo
  - Modo balanceo de carga y conmutación por error.
  - Modo VRRP
- Deberá incluir la capacidad de generar al menos 10,000 túneles VPN a través del protocolo IPSec.
- Deberá poder aplicar QoS (Quality of Service) para priorizar tráfico de Datos, Voz y Video
- Deberá poder crear políticas granulares es decir:
  - Para usuarios
  - Para grupos

Además deberá identificar, permitir, bloquear o limitar el uso de aplicaciones independientemente del puerto, protocolo o técnica evasiva.

- Deberá permitir el escaneo de aplicaciones tales como mensajería instantánea, redes sociales, streaming de video, Voz sobre IP, juegos entre otras.
- Deberá poder realizar autenticación de usuarios a través de Directorio Activo (LDAP), Portal Cautivo, Kerberos, Radius, Tacacs.
- Deberá contar con la administración centralizada de acceso a usuarios, a los recursos del Instituto y aplicaciones en Internet
- Deberá permitir la conexión a las aplicaciones del Instituto a través de dispositivos móviles (Tablet's, SmartPhone's)

4.4.2 *Soporte para la Operación de la Seguridad de la Nube IMSS*

Descripción del Servicio:

El Instituto requiere que el LICITANTE del servicio cuente con un Centro de Operaciones de la Seguridad (SOC) totalmente funcional en la actualidad, que se encuentre físicamente en las instalaciones del LICITANTE. El objetivo de este centro deberá ser la gestión de la seguridad y responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad, que ejecute actividades de revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, análisis forense, notificación de alertas y vulnerabilidades, así como el establecimiento de acciones de mejora sustentable.

Detalles del Servicio:

Ubicarse dentro de territorio mexicano (a fin de que se encuentre dentro de jurisdicción de las leyes mexicanas)

Contar con un mecanismo que garantice la continuidad de la operación frente a contingencias

Operación 7x24x365 días durante la vigencia del contrato.

Personal en sitio y remoto altamente calificado con las credenciales requeridas para la administración y monitoreo de los componentes que integran la solución.

Mantenimiento de las suscripciones a sitios y listas de correos de internet que alertan de nuevas vulnerabilidades.

Infraestructura dedicada para la administración, operación y monitoreo de los componentes hardware y software.

Revisión continúa a la configuración implementada en los dispositivos de seguridad. La finalidad es identificar errores, depurar reglas, optimizar el desempeño de los componentes hardware y software, así como mantener las configuraciones en cumplimiento con los requisitos de seguridad que establece la normatividad y estándares aplicables.

Acciones correctivas y preventivas para asegurar la confidencialidad, integridad y disponibilidad de la información.

Notificaciones y alertas personalizadas, en caso de desviaciones, anormalidades o brechas de seguridad.

Personal especializado en revisiones de seguridad en infraestructura y aplicaciones.

Revisiones continuas a la operación del SOC, que permitan establecer mejora en los procesos, procedimientos y controles de seguridad.

Atención y Respuesta a Incidentes de Seguridad.

Soporte y Atención a fallas a los componentes hardware y software que integran la solución.

Monitorear la disponibilidad de los componentes hardware y software que integran la solución ofertada. La solución de monitoreo debe tener la capacidad de generar alertas y notificaciones en caso de fallas, degradación de los signos vitales, intermitencia y/o pérdida de disponibilidad.

Mantenimiento preventivo y correctivo a la solución instalada.

Administración de Dispositivos.

Administración de Requerimientos.

Administración de Cambios.

Administración de Configuraciones.

Administración de Vulnerabilidades.

Administración de Incidentes.

Administración de Problemas.

Investigación de Incidentes.

Mesa de servicio apegada a ITIL v3.

El servicio de soporte a fallas deberá permitir el levantamiento de tickets a través de los siguientes medios:

- Número directo de las instalaciones del SOC.
- Correo Electrónico

El personal que el prestador del servicio integre y que se relaciona en puntos anteriores, deberá contar con experiencia probada en las áreas de tecnología y de seguridad de la información que se indica:

- Currículum vitae de todo el personal deberá indicar al menos:
- Experiencia profesional: bajo este rubro, se considerarán todos los cargos que cada integrante haya desempeñado, con fecha, nombre de los empleadores, nombre de los cargos que ha ejercido y el tipo de funciones bajo su responsabilidad.
- Experiencia en proyectos de su especialidad en Seguridad de la Información: bajo este rubro se citarán y describirán todos los proyectos que el integrante ha participado, y deberá contar con experiencia comprobable de cuando menos 2 años.
- Estudios: bajo este rubro se anotarán todos los estudios en materia de seguridad de la información, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica. Las certificaciones son de tecnología y/o de seguridad de tipo "vendor-neutral".
- Incluir la estructura del grupo de trabajo, indicando por cada perfil las responsabilidades y competencias.
- El Instituto podrá solicitar la revisión de la infraestructura de seguridad por un tercero en cualquier momento, durante la vigencia del contrato, a fin de dar certeza de la entrega del servicio.
- Generación de reportes derivados de la falla en algún componente de la infraestructura de seguridad, la cual deberá contener por lo menos:
  - Infraestructura afectada y servicios asociados
  - Causa raíz
  - Remediación o medidas compensatorias propuestas en tanto se identifica la causa raíz
  - Impacto e indisponibilidad del servicio afectado

Las credenciales y capacidades que deberán cubrir los recursos asignados al proyecto se indican en el apéndice correspondiente.

Consideraciones generales para los servicios de soporte del SSNI

4.4.2.1 Administración y soporte de componentes de seguridad

Como referencia de los servicios que son proporcionados actualmente, se puede consultar las especificaciones técnicas en el apéndice correspondiente.

ANEXOS
DIVISIÓN DE CONTRATOS

4.4.2.1.1 Firewall

Descripción del servicio:

El Instituto requiere de la seguridad y protección de control de acceso, bloqueo contra ataques dirigidos a las aplicaciones e inspección sobre los paquetes a nivel de aplicación para identificar patrones de tráfico anómalo. La infraestructura propuesta deberá ser de última generación y dedicada exclusivamente para las necesidades del Instituto y deberá cumplir el LICITANTE con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de habilitación de los Firewalls en la arquitectura de seguridad y comunicaciones.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

Llevar a cabo todas las tareas necesarias para la revisión de los equipos en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante. Siempre y cuando esté autorizado por el Instituto.

Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes o nubes.

Proporcionar el acceso a servicios ubicados en la capa de servidores del centro de datos (DMZs), realizando la gestión de acuerdo al esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

Realizar traducciones de direcciones IP homologadas para garantizar la seguridad de servidores.

Gestionar las reglas y objetos requeridos para la protección de los flujos del Instituto.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Firewalls relacionados para al menos:

- Cumplir las políticas de reglas de acceso a la información.
- Notificar sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución.
- Notificar aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el LICITANTE del servicio deberá realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades.

4.4.2.1.2 IPS

Descripción del servicio:

El Instituto requiere del servicio de protección perimetral basado en firmas y que identifiquen vulnerabilidades, para contener los intentos de obtener acceso a los recursos o servicios publicados en Internet o Intranet que pudieran afectar la operación de la organización, detectar accesos no autorizados y prevenir fugas de información. La infraestructura propuesta deberá ser nueva, de última generación y dedicada exclusivamente para las necesidades del Instituto y deberá cumplir con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de mejora en los Equipos ya existentes de Sistema de Prevención de Intrusos (IPS por sus siglas en inglés) en la arquitectura de seguridad y comunicaciones.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

Llevar a cabo todas las tareas necesarias para la revisión de los equipos en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante. Siempre y cuando esté autorizado por el Instituto.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Prevención de Intrusos relacionados para al menos:

- Cumplir las políticas de reglas de acceso a la información.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el LICITANTE del servicio deberá realizar la sustitución de componentes tecnológicos por otros de igual o mejores características/funcionalidades.

4.4.2.1.3 Anti-denegación de Servicios (DDoS)

Descripción del servicio:

El Instituto requiere de un servicio de protección contra ataques de Denegación de Servicio Distribuido que se encuentren basados en firmas y volúmenes de conexión altos. La infraestructura propuesta deberá ser de última generación y dedicada exclusivamente para las necesidades del Instituto y deberá cumplir con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

El LICITANTE deberá definir en conjunto con el Instituto la estrategia de mejora de los equipos de Anti-denegación de Servicios (DDoS) en la arquitectura de seguridad y comunicaciones.

El LICITANTE deberá habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

El LICITANTE deberá llevar a cabo todas las tareas necesarias para la revisión del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

El LICITANTE deberá acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

El LICITANTE deberá Integrar cada dispositivo hacia su respectiva consola de administración.

El LICITANTE deberá asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.

El LICITANTE deberá prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

El LICITANTE deberá atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

El LICITANTE deberá emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Anti-denegación de Servicios (DDoS) relacionados para al menos:

005

- Cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el LICITANTE del servicio deberá realizar la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

4.4.2.1.4 Redes Privadas Virtuales – VPN (C2S – S2S)

Descripción del servicio:

El Instituto requiere del Servicio de interconexión a través de Internet que permitan establecer comunicación desde localidades remotas para la transferencia de información a través de un canal cifrado.

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de mejora de los equipos para Redes privadas Virtuales – VPN en la arquitectura de seguridad y comunicaciones.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

Llevar a cabo todas las tareas necesarias para la revisión de los equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Gestionar el alta de accesos remotos debida y previamente autorizados por el Instituto a través de los mecanismos y personal que para ello designe este último.

Solicitar de manera mensual la lista de usuarios dados de baja de la organización y proceder a la deshabilitación de sus accesos remotos de manera inmediata.

Reportar bajo demanda la lista de usuarios y entidades (terceros) que cuentan con acceso remoto VPN C2S – S2S.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Redes privadas Virtuales – VPN relacionados para al menos:

- Cumplir las políticas de reglas de acceso a la información.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución, configuradas para las cuentas de usuario o servicios con terceros.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el LICITANTE del servicio deberá realizar la sustitución de componentes tecnológicos por otros de igual o mejores características/funcionalidades.

4.4.2.1.5 Gestión Unificada de Amenazas (UTM)

Descripción del servicio:

El Instituto requiere de un servicio de protección perimetral especializada en control de acceso, prevención de intrusos, Filtrado de Contenido Web y VPN, para control de tráfico y detección de actividad anómala. La infraestructura propuesta deberá ser de última generación y dedicada exclusivamente para las necesidades del Instituto y deberá cumplir con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

El LICITANTE deberá definir en conjunto con el Instituto la estrategia de mejora de los equipos de Gestión Unificada de Amenazas (UTM) en la arquitectura de seguridad y comunicaciones.

El LICITANTE deberá llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

El LICITANTE deberá acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

El LICITANTE deberá Integrar cada dispositivo hacia su respectiva consola de administración.

El LICITANTE deberá asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.

El LICITANTE deberá prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto

El LICITANTE deberá atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

El LICITANTE deberá emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Gestión Unificada de Amenazas (UTM) relacionados para al menos:

- Cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el LICITANTE del servicio deberá realizar la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

4.4.2.1.6 Filtrado de Contenido Web

Descripción del servicio:

El Instituto requiere del servicio de filtrado de contenido Web mediante políticas de acceso que permita controlar y filtrar la utilización del servicios de acceso a Internet, en función de roles y perfiles. La infraestructura propuesta deberá ser de última generación y dedicada exclusivamente para las necesidades del Instituto y deberá cumplir con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de mejora de los equipos de Filtrado de Contenido Web en la arquitectura de seguridad y comunicaciones.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

Llevar a cabo todas las tareas necesarias para la revisión de los equipos en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante. Siempre y cuando esté autorizado por el Instituto.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Filtrado de Contenido de Correo relacionados con al menos:

- Cumplir las políticas de reglas de acceso a la información.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución, configuradas para las cuentas de usuario.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución de Filtrado de Contenido Web, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

La solución ofertada deberá incluir el licenciamiento necesario para soportar 120,000 usuarios de manera simultánea.

Acordar con el Instituto el tipo de implementación que se integrará para el uso de los servicios (modo implícito o explícito), y en su caso, podrá solicitar modificaciones al uso del mismo conforme las necesidades operativas así lo demanden.

4.4.2.1.7 Antispam

Descripción del servicio:

El Instituto requiere del servicio de analizar correos electrónicos de entrada y salida con el objetivo de bloquear amenazas de spam, malware, phishing, amenaza persistente avanzada (Advanced Persistent Threat APT's), reputación de URLs embebidas en los correos. La infraestructura propuesta deberá ser de última generación y dedicada exclusivamente para las necesidades del Instituto y deberá cumplir con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de mejora de los equipos de Filtrado de Contenido de Correo Electrónico (Antispam) en la arquitectura de seguridad y comunicaciones.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

Llevar a cabo todas las tareas necesarias para la revisión del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante. Siempre y cuando esté autorizado por el Instituto.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Conocer y entender las políticas actuales de seguridad del Instituto, particularmente aquellas relacionadas con el manejo de información.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Filtrado de Contenido de Correo relacionados con al menos:

- Cumplir las políticas de reglas de acceso a la información.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución, configuradas para las cuentas de usuario.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución de Filtrado de Contenido de Correo, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el LICITANTE del servicio deberá realizar la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

4.4.2.1.8 Antimalware

Descripción del servicio:

El Instituto requiere de un servicio de detección y protección contra amenazas avanzadas en la red interna. La infraestructura propuesta deberá ser de última generación y dedicada exclusivamente para las necesidades del Instituto y deberá cumplir con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de mejora de los equipos de Antimalware en la arquitectura de seguridad y comunicaciones.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

Llevar a cabo todas las tareas necesarias para la revisión del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Antimalware relacionados para al menos:

- Cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución, configuradas para el tráfico externo y/o interno.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el LICITANTE del servicio deberá realizar la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

4.4.2.1.9 Firewall Especializado en Servicios Web (WAF)

Descripción del servicio:

El Instituto requiere del servicio de protección, prevención y control de ataques para aplicativos web expuestos en Internet. La infraestructura propuesta deberá ser de última generación y dedicada exclusivamente para las necesidades del Instituto y deberá cumplir con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de mejora de los equipos de Firewall Especializado en Servicios Web (WAF) en la arquitectura de seguridad y comunicaciones.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

Llevar a cabo todas las tareas necesarias para la revisión de los equipos en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Revisar y validar en conjunto con el Instituto los requerimientos de protección, inspección de contenido http o https y seguridad de aplicativos web tal y como sea solicitado.

Aprovisionar nuevos servicios aplicativos que requieran la protección a través del WAF, conforme el Instituto lo necesite, siempre y cuando las capacidades del equipo lo soporten, en cuyo caso el instituto solicitará una unidad de consumo adicional.

Integrar diseño, soporte de cambios y reingenierías en WAF.

Monitorear y optimizar el uso de los servicios de WAF.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Firewall Especializado en Servicios Web (WAF) relacionados para al menos:

- Cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución, configuradas para los servicios web públicos y/o privados.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el LICITANTE del servicio deberá realizar la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

4.4.2.2 Entregables de única ocasión

4.4.2.2.1 Centro de Operaciones de Seguridad (SOC)

- Diseño físico y lógico de alto nivel con la descripción detallada de la arquitectura propuesta para habilitar los servicios de la solución de seguridad.
- Copia de los siguientes procesos de seguridad que tiene implementados en el "SOC":
  - Proceso de Administración y Control de Cambios.
  - Proceso de Disponibilidad.
  - Proceso de Administración de Vulnerabilidades.
  - Proceso de Atención y Respuesta a Incidentes.
  - Proceso de Mejora Continua.

- La matriz de escalamiento del servicio tanto técnico como jerárquica.
- Procesos de la Mesa de Servicio, que se indican a continuación:
  - Administración de incidentes.
  - Administración de problemas.
  - Administración de cambios y configuraciones.
  - Administración de liberaciones.
- Metodología para el proceso de administración de vulnerabilidades.
- Procedimientos de seguridad aplicados en el "SOC" para:
  - Manejo de alarmas.
  - Atención y Respuesta a Incidentes de Seguridad

4.4.2.3 Entregables Periódicos

El LICITANTE deberá generar de manera integrada un **Entregable Mensual del Servicio de Seguridad**, que incluya de manera enunciativa más no limitativa los siguientes conceptos:

Servicios de Operación

4.4.2.3.1 Firewall

- Reporte de la disponibilidad de los activos de infraestructura (firewall), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (firewall), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (firewall), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (firewall), incluyendo tiempos de solución.
- Reporte de promedio de tráfico de entrada/salida por cada DMZ asignada.
- Reporte del top diez (10) de los protocolos bloqueados.
- Reporte del top diez (10) de los protocolos permitidos.
- Reporte de reglas de control de acceso más utilizadas.
- Reporte del top diez (10) de direcciones IP Públicas/Privadas con más consumo de ancho de banda.

4.4.2.3.2 IPS

- Reporte de la disponibilidad de los activos de infraestructura (IPS), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (IPS), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (IPS), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (IPS), incluyendo tiempos de solución.
- Reporte de promedio de tráfico de entrada/salida.
- Reporte del top diez (10) de intentos ataques detectados y bloqueados (firmas).
- Reporte del top diez (10) de equipos que generar tráfico anómalo.
- Reporte del top diez (10) de usuarios que generan tráfico anómalo.

4.4.2.3.3 Anti-denegación de Servicios (DDoS)

- Reporte de la disponibilidad de los activos de infraestructura (AntiDDoS), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.

- Reporte de los controles de cambios en de los activos de infraestructura (AntiDDoS), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (AntiDDoS), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (AntiDDoS), incluyendo tiempos de solución.
- Reporte del top diez (10) de anomalías clasificadas por nivel de severidad.
- Reporte del top diez (10) de activos de infraestructura con mayor número de incidencias de tráfico anómalo (internos/externos).
- Reporte del top diez (10) de protocolos bloqueados.

4.4.2.3.4 Redes Privadas Virtuales – VPN (C2S – S2S)

- Reporte de la disponibilidad de los activos de infraestructura (Concentrador VPN), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (Concentrado VPN), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (Concentrador VPN), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (Concentrador VPN), incluyendo tiempos de solución.
- Reporte del top diez (10) usuarios que se conectan a través de VPN C2S.
- Reporte del top diez (10) de servicios (direcciones IP destino) que se conectan a través de VPN C2S y S2S.
- Reporte del top diez (10) de ancho de banda consumido por VPN S2S.

4.4.2.3.5 Gestión Unificada de Amenazas (UTM)

- Reporte de la disponibilidad de los activos de infraestructura (UTM), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (UTM), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (UTM), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (UTM), incluyendo tiempos de solución.
- Reporte del top diez (10) de los protocolos bloqueados.
- Reporte del top diez (10) de los protocolos permitidos.
- Reporte del top diez (10) de intentos ataques detectados y bloqueados (firmas).
- Reporte del top diez (10) de equipos que generar tráfico anómalo.
- Reporte del top veinte (20) sitios web bloqueados.
- Reporte del top veinte (20) sitios web permitidos.
- Reporte del top veinte (20) de IP/Usuarios con mayor navegación a Internet.
- Reporte del top diez (10) de servicios (direcciones IP destino) que se conectan a través de VPN.

4.4.2.3.6 Filtrado de Contenido Web

- Reporte de la disponibilidad de los activos de infraestructura (Filtrado de Contenido Web), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (Filtrado de Contenido Web), incluyendo tiempo de atención.

- Reporte de incidentes atendidos en los activos de infraestructura (Filtrado de Contenido Web), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (Filtrado de Contenido Web), incluyendo tiempos de solución.
- Reporte del top veinte (20) sitios web bloqueados.
- Reporte del top veinte (20) sitios web permitidos.
- Reporte del top veinte (20) categorías bloqueadas.
- Reporte del top veinte (20) categorías permitidas.
- Reporte del top veinte (20) de IP/Usuarios con mayor navegación a Internet.
- Reporte del top veinte (20) de IP/Usuarios con mayor consumo de ancho de banda.

4.4.2.3.7 Antispam

- Reporte de la disponibilidad de los activos de infraestructura (Antispam), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (Antispam), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (Antispam), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (Antispam), incluyendo tiempos de solución.
- Estadísticas de correos electrónicos bloqueados y recibidos.
- Reporte del top diez (10) de usuarios con mayor recepción de correo electrónico.
- Reporte del top diez (10) de usuarios con mayor envió de correo electrónico.
- Reporte del top diez (10) de dominios bloqueados (entrada/salida).
- Reporte del top diez (10) de dominios permitidos (entrada/salida).
- Reporte del top diez (10) de tamaño de información transferida por correo electrónico (entrada/salida).
- Reporte del top diez (10) de virus identificados.

4.4.2.3.8 Antimalware

- Reporte de la matriz de riesgos a partir de los hallazgos encontrados.
- Reporte de tabla de hallazgos clasificados por su riesgo donde se integren los hallazgos encontrados indicando el número de eventos asociados y el impacto que estos causan.
- Reporte del inventario de los sistemas operativos monitoreados.
- Reporte con el detalle técnico de cada incidente detectado, y que integre:
  - Fecha y hora del incidente.
  - Dirección IP de origen, destino, puerto de origen y destino.
  - Dispositivos asociados con el incidente.
  - Usuario de directorio activo presente durante el momento del incidente (si aplica).
  - Clasificación del incidente.
  - Origen del ataque y destino del atacante (en caso de aplicar).
  - Sistema operativo origen.

4.4.2.3.9 Firewall Especializado en Servicios Web (WAF)

- Reporte de la disponibilidad de los activos de infraestructura (WAF), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (WAF), incluyendo tiempo de atención.

- Reporte de incidentes atendidos en los activos de infraestructura (WAF), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (WAF), incluyendo tiempos de solución.
- Reporte del top diez (10) de ataques bloqueados.
- Reporte del top diez (10) de portales con más ataques.
- Reporte de top diez (10) de consumo de ancho de banda.

4.4.2.4 Entregables bajo demanda:

El LICITANTE generará bajo demanda los siguientes documentos y/o reportes, a solicitud del órgano de gobierno que señale el Instituto; y que incluyen de manera enunciativa más no limitativa los siguientes conceptos:

4.4.2.4.1 Servicios de Control de Calidad

4.4.2.4.1.1 *Análisis de Vulnerabilidades*

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados, así como el plan de mitigación propuesto.
- Archivos electrónicos (MS Excel) con la información fuente obtenida de las herramientas tecnológicas que se utilizaron para realizar los escaneos de vulnerabilidades.
- Reporte de los escaneos de vulnerabilidades realizados, indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja).

4.4.2.4.1.2 *Pruebas de Penetración*

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura verificados, así como el plan de mitigación propuesto.
- Archivos electrónicos (MS Excel) con la información fuente obtenida de las herramientas tecnológicas que se utilizaron para realizar las pruebas de penetración.
- Reporte de las pruebas de penetración realizadas, indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de ejecución, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja).

4.4.2.4.1.3 *Análisis Forenses*

Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle del análisis forense ejecutado por cada activo o grupo de activos de infraestructura verificados.

4.4.2.4.1.4 *Borrado Seguro de Datos*

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro por cada activo o grupo de activos de infraestructura eliminados.
- Archivos electrónicos (Html y PDF) con la información fuente obtenida de las herramientas tecnológicas que se utilizaron para realizar los borrados seguros de la información.
- Reporte mensual de los borrados seguros realizados, indicando al menos: Activo(s) de infraestructura, fecha de eliminación.

4.4.2.4.1.5 *Análisis de Riesgos de Seguridad de la Información*

- Reporte ejecutivo en formato electrónico (MS Word, PDF) de la actividad de Análisis de Riesgos que incluya:
  - Identificación activos, considerando como activos a los procesos, actividades, información, infraestructura, y gente.
  - Identificación de vulnerabilidades.
  - Identificación de amenazas.
  - Escenarios de riesgo.
  - Priorización del riesgo.

4.4.2.4.1.6 *Sistema de Gestión de Seguridad de la Información (SGSI)*

- Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora del Sistemas De Gestión de Seguridad de la Información que incluya:
  - Capacitación inicial
  - Generación de directivas de seguridad
  - Identificación y valuación de activos
  - Generación de la Declaración de Aplicabilidad
  - Generación del plan de tratamiento de riesgos
  - Propuestas de implementación de los controles
  - Manual de Gestión de Seguridad de la Información

Los reportes y/o documentos anteriores deberán ser entregados en el formato y fecha que hayan sido acordados con el órgano de gobierno del Instituto que los haya solicitado; y deberán ser integrados al **Entregable Mensual del Servicio de Seguridad)** en el periodo que corresponda a su entrega, para la validación de los niveles de servicio que correspondan.

4.4.2.5 Consideraciones generales para la entrega de los servicios de seguridad

El **LICITANTE** deberá:

Fortalecer la seguridad de la información de la Institución contra amenazas, disminuyendo el riesgo de sufrir incidentes de seguridad, mediante el uso de tecnología de punta para el monitoreo, detección, aseguramiento, y contención de ataques que puedan presentarse en la infraestructura de cómputo, sistemas y aplicaciones del Instituto.

Contar con servicios de infraestructura regulados por niveles de servicio, que: implementen (instalen, migren, habiliten y pongan a punto) los componentes necesario en los Centros de Datos del Instituto, u otras localidades que este último designe, y que de forma complementaria gestionen (operen, monitoreen, den soporte y mantenimiento preventivo y correctivo) a la correspondiente infraestructura con el propósito de satisfacer las necesidades de: conectividad, comunicación, protección, control y filtrado de la propia Institución, manteniendo la plataforma tecnológica en condiciones óptimas de operación.

Contar con los servicios de protección de forma unificada e integrada, incluyendo protección de servidores, conectividad, navegación, filtrado, entre otros; mediante una solución integral que permita una gestión

0057

consolidada de las funcionalidades, características y servicios, con el propósito de mantener y robustecer el esquema de seguridad del Instituto.

Contar con servicios de seguridad de la información, que complementen el esquema de seguridad institucional de forma consistente y robusta, con el control, aseguramiento, diagnóstico, protección, pruebas, metodologías, de distintos rubros como el de acceso a cuentas privilegiadas, base de datos, aplicaciones, fuentes múltiples, vulnerabilidades, investigación forense y de procesos de seguridad, así como con otros servicios especializados en materia de seguridad y tecnologías de la información.

Efectuar la actualización de cualquier tipo de licencia, componente, dispositivo, parche, arquitectura, etc. siempre y cuando el fabricante de dicho componente haya liberado una versión que lo reemplace por aspectos de seguridad, compatibilidad, error o falla detectada, o similar; con la finalidad de mantener estable y segura la operación de los servicios del Instituto, entendiendo que toda actualización o mejora debe ser consultada y aprobada por este último.

Garantizar la operación, licenciamiento, soporte técnico, mantenimiento correctivo y preventivo, así como el reemplazo de partes (por parte del fabricante del componente o de la solución), de los servicios propuestos, considerando la cantidad de unidades de licenciamiento como los dispositivos, los usuarios concurrentes, entre otros, conforme la naturaleza y características del servicio que dicha infraestructura y base instalada soportan.

Integrar a los servicios de gestión, operación, soporte y mantenimiento provistos por su Centro de Operaciones de Seguridad (SOC) para los servicios ofrecidos, dando cumplimiento a las condiciones del presente contrato.

Establecer Mesas de trabajo con el Instituto, a fin de llevar a cabo la planeación para la toma de operación de la infraestructura y base instalada, con el propósito de no afectar la continuidad operativa, de negocios o de seguridad de este último.

Poner en marcha los servicios de su Centro de Operaciones de Seguridad (SOC), así como establecer los enlaces de comunicaciones que los interconecten con la red de Gestión del Instituto previo a la transición a la operación del servicio.

Establecer su Mesa de Servicio, para lo cual, durante la fase de toma de operación y transición, deberá tener ya disponible un servicio de Mesa de Servicio.

Proporcionar la información relacionada con la documentación que soportan los servicios, incluyendo entre otros, memorias técnicas, manuales y/o procedimientos de atención de servicios, matrices de escalamiento que permitirán al Instituto validar en cualquier momento los elementos que componen los diversos servicios.

ANEXOS
DIVISIÓN DE CONTRATOS

4.4.3 *Consumo de BCFs y BCCs para el servicio de seguridad*

El SSNI podrán consumir BCFs y BCCs que se encuentren disponibles según lo que se describe en este mismo apartado "Servicio de Operación y Calidad de la Seguridad Informática Perimetral" para todas las modalidades de despliegue, conforme a lo que se especifica en la sección "3.6 Elementos comunes de los Servicios", será responsable de validar su consumo y disponibilidad valiéndose de la información de que proporcionen sus propios servicios de "Soporte para la Calidad de la Seguridad de la Nube IMSS" y "Soporte para la Operación de la Seguridad de la Nube IMSS".

4.4.4 *Servicios eventuales de seguridad*

A lo largo del servicio de Soporte para la Calidad de la Seguridad de la Nube IMSS y de Soporte para la Operación de la Seguridad de la Nube IMSS, se señalan una serie de servicios que pueden ser consumidos de manera eventual. Dichos servicios serán cotizados de manera individual según se señala en la sección Catálogo de Servicios.

4.4.5 *Servicios extendidos*

Conforme a lo señalado en la sección Elementos comunes de los Servicios, los servicios extendidos se derivan del servicio de Soporte para la Calidad de la Seguridad de la Nube IMSS y del servicio de Soporte para la Operación de la Seguridad de la Nube IMSS.

4.5 Servicio de Gestión de Medición del Desempeño de Aplicativos y Componentes Institucionales

El **LICITANTE** deberá incluir en su propuesta que proporcionará al Instituto el servicio descrito en la presente sección, para el cual se deberán incluir las siguientes fases: a) diagnóstico inicial del estado de aplicativos y componentes Institucionales, b) optimización del estado actual para mejora del desempeño óptimo y, c) propuesta para su implementación en un estado mínimo funcional. A partir del desarrollo de las fases antes indicadas, el Instituto determinará y notificará al Licitante ganador si es requerido probar las fases antes descritas, considerando para ello, la infraestructura que el Instituto determine.

El **LICITANTE** deberá incluir en su propuesta que se apegará al marco tecnológico de referencia y a los lineamientos Institucionales establecidos para aplicativos, software, componentes, infraestructura, telecomunicaciones y seguridad, para la entrega de componentes, servicios e infraestructura que permitan efectuar las pruebas de medición de desempeño en el Centro de Datos Institucional o en otro Centro de Datos que el Instituto designe para tal efecto.

Así mismo, el **LICITANTE** deberá apegarse al marco tecnológico de referencia y a los lineamientos Institucionales establecidos para aplicativos, software, componentes, infraestructura, telecomunicaciones y seguridad, para la entrega de componentes, servicios e infraestructura que permitan efectuar las pruebas de medición de desempeño en el Centro de Datos del **LICITANTE** que resulte adjudicado o en otro Centro de Datos que el Instituto designe para las pruebas.

El **LICITANTE** deberá incluir en su propuesta la posibilidad de atención bajo demanda por parte del Instituto, que realizará el análisis y desarrollo solicitado para atender requerimientos de Nivel Central y en caso de así solicitarlo en Instituto, de las 35 oficinas de representación institucional, permitiendo al Instituto el

cumplimiento de objetivos, metas y diferentes requerimientos por parte de entidades fiscalizadoras cuando así lo soliciten.

El **LICITANTE** deberá ofertar, detallar y describir en su propuesta que el servicio requerido por el Instituto incluirá por lo menos los siguientes elementos:

4.5.1 De la fase de diagnóstico inicial del estado de aplicativos y componentes Institucionales:

- El **LICITANTE** deberá considerar la información con la que actualmente operan los aplicativos institucionales en el centro de datos tercerizado para cada aplicativo o componente que el Instituto determine. Este análisis deberá ser documentado con base en la infraestructura usada en la actualidad y considerando en todo momento lo siguiente: licenciamiento, servidores, manejadores de bases de datos, almacenamiento, telecomunicaciones y otros componentes de infraestructura que sean necesarios para la operación actual; así mismo las interdependencias con otros aplicativos, componentes transversales, propios del Instituto y externos.
- El **LICITANTE** deberá realizar y proveer de diagramas de arquitectura tecnológica detallados, la descripción precisa y las capacidades actuales de cada activo de información utilizado dentro de la infraestructura del centro de datos tercerizado, así mismo y hasta donde sea posible, de los componentes transversales utilizados en cada aplicativo y otras interdependencias.
- El **LICITANTE** deberá generar los documentos y reportes requeridos por el Instituto con la intención de presentar avances y resultados de esta fase y las actividades asociadas.
- Es importante mencionar que el **LICITANTE** deberá entregar un diagnóstico completo para que el Instituto tenga información detallada y que dé una visión completa acerca del estado actual de operación de los aplicativos o componentes seleccionados por el Instituto.

Entregables de esta fase:

- El entregable de esta fase consiste en un informe que incluya: el plan de trabajo, los diagramas de arquitectura tecnológica con todos los activos de información relacionados, su respectiva descripción, incluyendo el estado actual de capacidades tecnológicas y comportamiento del aplicativo o componente hasta donde sea posible.
- Además, el **LICITANTE** deberá realizar la debida transferencia de conocimiento para la *Gestión de Medición del Desempeño*, identificando la operación colaborativa con el personal designado por el Instituto, para la aplicación de la estrategia desarrollada e implementada, considerando en esta los cambios organizacionales cuando ocurran.
- El **LICITANTE** trabajará en conjunto con el Instituto para comunicar y entrenar a los servidores públicos relacionados con esta fase, acerca de sus roles y responsabilidades, para cumplir lo establecido en los objetivos de esta, de acuerdo con los planes de trabajo desarrollados.
- Finalmente, se dará por concluida esta fase, una vez que haya sido aceptado y firmado el entregable, conforme al alcance y actividades propuestas por el **LICITANTE** y autorizadas por el personal que el Instituto designe.

4.5.2 De la fase de optimización del estado actual para mejora del desempeño óptimo:

- A partir del resultado de la fase anterior, El **LICITANTE** deberá identificar y actualizar los cambios de o hacia los activos de información que componen la operación de los aplicativos o componentes Institucionales seleccionados, ubicados y utilizados en la infraestructura propiedad del Instituto, la del centro de datos tercerizado hasta donde sea posible y, de sus socios comerciales.

- El **LICITANTE** deberá hacer una medición de capacidades actuales de: los recursos, los servicios y los procesos, que permitan aislar y optimizar la operación del aplicativo o componente seleccionado por el Instituto, priorizando las características de eficiencia y eficacia.
- En este análisis, el **LICITANTE** deberá determinar los niveles de desempeño óptimo del aplicativo o componente comparado con el estado actual, previa validación por el personal designado por el Instituto.
- El **LICITANTE** deberá documentar todas y cada una de las actividades realizadas; se dará por concluida esta fase, una vez que haya sido aceptado y firmado el entregable, conforme al alcance y actividades propuestas por el **LICITANTE** y autorizadas por el personal que el Instituto designe.

Entregables de esta fase:

- El entregable de esta fase consiste en un informe que incluya: la mejora del aplicativo o componente seleccionado considerando las características de eficiencia y eficacia, justificando minuciosamente las mejoras propuestas y realizando un comparativo del estado actual con esta.
- Además, el **LICITANTE** deberá incluir en su propuesta que realizará la debida transferencia de conocimiento para la *Medición del Desempeño Óptimo*, identificando la operación colaborativa con el personal designado por el Instituto, para la aplicación de la estrategia desarrollada e implementada, considerando en esta los cambios organizacionales cuando ocurran.
- El **LICITANTE** deberá incluir en su propuesta que trabajará en conjunto con el personal del Instituto para comunicar y entrenar a los servidores públicos relacionados con esta fase, acerca de sus roles y responsabilidades, para cumplir lo establecido en los objetivos de esta, de acuerdo con el plan de trabajo desarrollado.
- Finalmente, se dará por concluida esta fase, una vez que haya sido aceptado y firmado el entregable, conforme al alcance y actividades propuestas por el **LICITANTE** y autorizadas por el personal que el Instituto designe.

4.5.3 De la fase de propuesta para su implementación en un estado mínimo funcional:

- El **LICITANTE** deberá incluir en su propuesta, que, considerando el resultado de la fase anterior, deberá presentar una propuesta para la reducción del ecosistema del aplicativo o componente Institucional seleccionado.
- El **LICITANTE** que resulte adjudicado deberá hacer una medición de los recursos, los servicios y los procesos mínimos necesarios, que permitan poner en operación el aplicativo o componente seleccionado por el Instituto, priorizando las características de eficiencia, eficacia y austeridad.
- En esta fase, el **LICITANTE** que resulte adjudicado deberá presentar los niveles de desempeño necesarios del aplicativo o componente en su versión mínima, previa validación por el Instituto.
- El **LICITANTE** que resulte adjudicado deberá documentar todas y cada una de las actividades realizadas; se dará por concluida esta fase, una vez que haya sido aceptado y firmado el entregable, conforme al alcance y actividades propuestas por el **LICITANTE** que resulte adjudicado y autorizadas por el personal que el Instituto designe.
- El **LICITANTE** que resulte adjudicado realizará un flujo de trabajo de su propuesta, considerando las relaciones e interdependencias del aplicativo o componente seleccionado con otros, propios del Instituto o relacionados con otras Instituciones y socios comerciales, llevará a cabo la presentación del flujo de trabajo y de la documentación de este, considerando los resultados y nuevos hallazgos o mejoras identificados durante su presentación.
- El servicio se solicitará y ejecutará bajo demanda, considerando las necesidades de cumplimiento con las autoridades correspondientes y necesidades del Instituto.

- El **LICITANTE** que resulte adjudicado deberá entregar el flujo de trabajo final que permita al Instituto la ejecución de las pruebas de laboratorio de medición del desempeño del aplicativo o componente seleccionado.

Entregables de esta fase:

- El entregable de esta fase consiste en un informe que incluya: la propuesta del flujo de trabajo detallada, para el aplicativo o componente Institucional en su versión mínima y completamente funcional; es decir, que permita cumplir con la naturaleza de su desarrollo y puesta en marcha.
- El informe deberá integrar una metodología y su respectivo plan de trabajo general, que permita al Instituto y en caso de ser requerido, la ejecución de las pruebas de laboratorio de medición del desempeño del aplicativo o componente seleccionado.
- El **LICITANTE** que resulte adjudicado deberá realizar la debida transferencia de conocimiento del flujo de trabajo para la ejecución de las pruebas del *Laboratorio de Medición del Desempeño en su versión mínima y funcional*, identificando la operación colaborativa con el personal designado por el Instituto, para la aplicación de la estrategia desarrollada e implementada, considerando en esta los cambios organizacionales cuando ocurran.
- El **LICITANTE** que resulte adjudicado trabajará en conjunto con el Instituto para comunicar y entrenar a los servidores públicos relacionados con esta fase, acerca de sus roles y responsabilidades, para cumplir lo establecido en los objetivos de esta de acuerdo al plan de trabajo desarrollado.
- Finalmente, se dará por concluida esta fase, una vez que haya sido aceptado y firmado el entregable, conforme al alcance y actividades propuestas por el **LICITANTE** y autorizadas por el personal que el Instituto designe.

4.6 Elementos comunes de los Servicios

4.6.1 Servicio de Infraestructura y Bloques de Construcción Fundamentales.

El **LICITANTE** deberá aprovisionar cualquiera de los BCF establecidos en el apéndice "Bloques de Construcción" en la modalidad de Infraestructura como Servicio. En dicho apéndice se describen los distintos tipos de componentes considerados como BCF a los cuales el Instituto podrá tener acceso durante la vigencia del contrato.

El dominio de aplicaciones incluye dos áreas: sistemas y componentes de aplicaciones; los cuales vienen empaquetados y son autocontenidos y se refieren exclusivamente al software, por lo que se deben integrar con los BCFs de Infraestructura descritos más adelante.

- Los sistemas son conjuntos discretos de recursos de información, organizados para la recolección, procesamiento, mantenimiento, uso, distribución, difusión o disposición de información para sustentar un proceso de negocio específico del Instituto; y se incluyen las siguientes categorías, de manera enunciativa más no limitativa:
  - Sistemas de gestión de adquisiciones
  - Gestión financiera
  - Administración del personal
  - Gestión de recursos humanos
  - Gestión de activos y propiedades
  - Gestión de la seguridad
  - Gestión de los sistemas

- Los componentes de aplicación corresponde al software autocontenido mismo que podrá ser agregado o configurado para sustentar diferentes capacidades; y se incluyen las siguientes categorías, a manera de referencia:
    - Análisis, reporteo y estadísticas
    - Gestión de datos
    - Herramientas y entorno de desarrollo
    - Gestión de documentos y contenidos
    - Descubrimiento y gestión del conocimiento
    - Middleware
    - Automatización y gestión de procesos
    - Productividad
    - Controles de seguridad
    - Comunicación unificada y colaboración
    - Visualización
    - Acceso Web

El dominio de infraestructura tiene por objeto proporcionar un esquema de categorización para los activos físicos de TI, los sistemas operativos y firmware que los controlan, y los lugares o instalaciones que albergan los activos de TI físicos. Se divide en tres áreas, Plataforma, Red e Instalaciones, que están vinculados y relacionados entre sí para permitir el análisis de los activos de TI a través de las tres dimensiones.

- La plataforma incluye la arquitectura de hardware y el marco de trabajo para el software, donde la combinación permite que el software pueda ejecutarse, en particular software de aplicación. La plataformas incluyen la arquitectura de computadoras, el sistema operativo y los dispositivos internos; así como plataformas de software que emulan las plataformas de hardware completas (por ejemplo, la virtualización del sistema); y se incluyen las siguientes categorías, a manera de referencia:
    - Hardware
    - Sistema operativo
    - Hardware de telecomunicaciones
    - Dispositivos periféricos
    - Virtualización
    - Nodo de Extensión de Nube Privada (ENP)
- La red describe los Bloques de Construcción Fundamentales que permiten acceder a un BCF o BCC en particular, utilizado dentro de los servicios del presente anexo técnico; y se incluyen las siguientes categorías, a manera de referencia:
    - Zona
    - Tipo de red
    - Infraestructura
    - Tipo de transmisión
- Las instalaciones proporciona el esquema de categorización para describir cómo y/o donde un BCF o BCC determinado será instalado, desplegado, y operado (para efectos de este Anexo Técnico, se corresponden con las modalidades de despliegue mencionadas anteriormente); y se incluyen las siguientes categorías, a manera de referencia:
    - Nodos de Extensión de Nube Privada (ENP)
    - Ambientes no productivos
    - Centro de Datos externo (Centro de Datos Primario)
    - Nodos de Extensión de la Nube Híbrida (ENH) del IMSS
    - Instalaciones designadas por el Instituto

Los BCF, sus características, versiones y especificaciones técnicas se encuentran dentro del Apéndice "1.Bloques de Construcción". Es importante señalar que tales BCF serán proporcionados como Servicios Administrados por lo que deberán contar de manera integral con todos los servicios de Soporte y Operación asociados a los mismos conforme a lo especificado en el presente Anexo Técnico.

4.6.2 Servicio de Plataformas y Bloques de Construcción Comunes.

4.6.2.1 Bloques de Construcción Comunes

Un Bloque de Construcción Común representa un grupo de componentes que son relevantes tecnológica y operativamente en su conjunto para una o más soluciones para el Instituto. Incluyen colecciones de capacidades y requerimientos comunes a diferencia de aquellos particulares de los de una solución específica, proveen estructuras con ambientes operativos específicos para las necesidades operativas y de información en la construcción de soluciones de negocio particulares.

Por solicitud del Instituto se declararán Bloques de Construcción Común definidos entre el Instituto y el **LICITANTE**. Una vez declarados los Bloques de Construcción Común, se tendrá un precio por BCC y en lo sucesivo se devengará por BCC y no por BCF. Así mismo, los niveles de servicio será medido por BCC y no por BCF por lo que las penas convencionales y deductivas que apliquen, serán aplicadas al BCC.

El **LICITANTE** en conjunto con el Instituto definirá un tiempo máximo para la habilitación de BCFs como BCC. En caso de que el **LICITANTE** no habilite el BCC en el plazo acordado, aplicarán las penas convencionales generales que establece el presente Anexo Técnico.

4.6.3 Servicios Extendidos de Soporte

El servicio de Soporte Extendido se contratará bajo demanda y se ejercerá a partir de las Unidades de Soporte Extendido, cada solicitud de proyecto recibirá un tratamiento individual por parte del **LICITANTE**.

4.6.3.1 Descripción del Servicio

El costo unitario de las Unidades de Soporte Extendido se calculará con base en la propuesta económica del **LICITANTE**, en los términos siguientes:

- Para las Unidades de Soporte Extendido para el **Servicio de Soporte para la Integralidad y Telecomunicaciones** será del 5% del costo unitario mensual del servicio.
- Para las Unidades de Soporte Extendido para el **Servicio de Seguridad** será del 5% del costo unitario mensual del servicio.
- Para las Unidades de Soporte Extendido para el **Servicio de Continuidad de la Operación y Soporte** será del 5% del costo unitario mensual del servicio.

Los servicios que estarán a cargo del **LICITANTE** para cada una de las Unidades de Soporte Extendido serán los necesarios para cumplir con los objetivos y alcance del Proyecto-Servicio.

ANEXOS
D[illegible]N DE CONTRATOS

4.6.3.2 Requisitos del Servicio

Los servicios o proyectos solicitados a través de esta modalidad tienen carácter de finitos en el tiempo y serán correctamente acotados en alcance conforme a la documentación que se señala a continuación. Para cada solicitud de Proyecto-Servicio que efectúe el Instituto a través de un Administrador del Contrato Respectivo, el **LICITANTE** será responsable de definir al menos, por escrito, con papel membretado de su empresa y firmado por el Representante Legal de la misma, los siguientes elementos con lujo de detalle:

1. Objetivos del Proyecto-Servicio
2. Alcances del Proyecto-Servicio
3. Actividades a realizar (Plan de Trabajo Detallado) que incluya fechas compromiso para los distintos entregables
4. Desglose técnico de los componentes que integren el servicio a prestar
5. Memoria técnica de los servicios (Información anexa de soporte, documentación y apoyo)
6. Justificación técnica de la correspondencia del objetivo del proyecto o servicio con las Unidades de Soporte Extendido de conformidad con el alcance técnico del mismo.

El costo unitario de estos servicios se derivan de la propuesta económica del **LICITANTE**. Estos servicios no forman parte de la propuesta económica y son adicionales dentro del monto máximo del contrato que resulte del presente proceso. Los posibles **LICITANTES** deberán incluirlos en su propuesta técnica con la afirmación de prestarlos en los términos descritos.

4.6.3.3 Mecanismo de consumo de las Unidades de Soporte Extendido

A continuación se muestran ejemplos de manera enunciativa más no limitativa y como referencia de los Proyectos-Servicios posibles a solicitar con las Unidades de Soporte Extendido de conformidad a la justificación técnica evaluada entre el **LICITANTE** y el Instituto, los siguientes:

a. Análisis de incorporación de servicios no previstos en este Anexo Técnico
b. Análisis de integración de servicios de comunicaciones, voz, video o datos pertenecientes a dominios ajenos a los servicios del presente anexo técnico.
c. Labores específicas de apoyo al instituto y al GGC en procesos no definidos en este Anexo Técnico.
d. Consultoría de descubrimiento y documentación detallada de estado actual de otros servicios de tecnologías de información y comunicaciones (TIC), así como de servicios de datos, voz, imagen, comunicaciones unificadas, video y otros relacionados.
e. Trabajos tendientes a la homogenización de servicios TIC, dentro de los cuales pudiera incluirse la provisión de servicios administrados.
f. Análisis y definición técnica de casos de uso de negocio para la interpretación de tráfico, de datos, de servicios digitales y electrónicos bajo la administración del IMSS.

4.6.3.4 Modalidad de Soporte Extendido

Cada servicio deberá recibir un tratamiento individual por parte del **LICITANTE**, para lo cual designará a un **Coordinador de Proyecto de Soporte Extendido** por solicitud, quien será responsable del seguimiento y control de la solicitud hasta su finalización. Dicho coordinador deberá asistir a las reuniones requeridas por el Instituto para determinar el alcance del proyecto, así como dar el seguimiento al mismo hasta su conclusión.

0961

Todo el personal designado por el **LICITANTE** para atender un proyecto o servicio de soporte extendido, no podrá pertenecer a los grupos que brindan cualquiera de los servicios descritos en el resto de los apartados del presente Anexo Técnico (salvo que se demuestre que es indispensable para el proyecto y en cuyo caso no deberán incluirse sus horas en la cotización, a menos que se demuestre que será reemplazado por alguien más en las funciones que generalmente realiza, sin menoscabo o riesgo del servicio en el que participa); y deberán contar con certificación o experiencia equivalente y comprobable para la prestación de los servicios a los que sean asignados, siendo en todo momento prerrogativa del Instituto la aceptación previo al inicio del servicio, de la persona y/o grupo de trabajo que participan, reservándose el derecho de solicitar el cambio del personal o recursos asignados al proyecto.

4.6.3.5 Consideraciones generales para la entrega de servicios extendidos

A continuación se señalan de manera enunciativa, más no limitativa, los proyectos y servicios que el Instituto identifica como de soporte extendido, entendiendo que dichos servicios pueden o no ser requeridos a través del Grupo de Gobierno del Contrato, durante la vida del contrato, sin menoscabo de que sean requeridos cualquier otro proyecto o servicio relacionado con los servicios administrados descritos en el presente Anexo Técnico:

- Servicios especializados de arquitectura, administración y soporte técnico no previstos en el Anexo Técnico con motivo de nuevos requerimientos y/o nuevas tecnologías requeridas por el Instituto relacionados al objeto del presente anexo técnico.
- Servicios de Análisis de integración de proyectos y/o servicios pertenecientes a nuevos dominios tecnológicos requeridos para la continuidad de los servicios considerados en el presente Anexo Técnico.

Servicios específicos de apoyo al Grupo de Gobierno de Contrato en relación a nuevos procesos, herramientas o mecanismos de operación y control no definidos en éste Anexo Técnico y que sean necesarios para mejorar el desempeño de los servicios del contrato.

5. PLAN DE ASEGURAMIENTO DE LA CALIDAD

5.1. CONDICIONES GENERALES

El **LICITANTE** deberá proveer de los insumos y equipos necesarios para ofrecer el servicio. Los incidentes y solicitudes deberán gestionarse para su atención a través de una mesa de servicios o centro de operaciones del **LICITANTE**. Todo el servicio técnico preventivo, correctivo, así como partes, refacciones y consumibles deberán ser incluidos como parte del servicio.

El **LICITANTE** ejecutará las acciones que permitan tener la calidad necesaria y garantizar la confidencialidad, integridad y disponibilidad requerida de los servicios que se describen en el presente anexo.

El **LICITANTE** de servicios deberá monitorear el estado de los equipos y servicios de tal manera que se generen acciones proactivas para corregir fallas sobre procesamiento, almacenamiento, red de telecomunicaciones, seguridad y servicios de voz, de la cual se proporciona la arquitectura actual.

El **LICITANTE** deberá contar con experiencia comprobable en la implementación y puesta a punto de servicios especificados en el presente anexo que garanticen la continuidad de los servicios del Instituto, y certificaciones tanto de la infraestructura y el personal del **LICITANTE** en las tecnologías ofertadas. Así

ANEXOS
DIVISIÓN DE CONTRATOS

mismo, demostrar mediante contratos similares (al menos 3) mediante una copia legible de contratos, pedidos y/o cartas del cumplimiento de proyectos de la misma naturaleza.

El **LICITANTE** deberá incluir un administrador de proyectos certificado en Project Manager Professional (PMP) por el Project Management Institute (PMI). Así mismo deberá presentar su certificación vigente durante la vigencia del contrato.

El centro de datos ofertado por el **LICITANTE** deberá estar certificado por el UPTIME INSTITUTE con el nivel de TIER III, el cual se utilizará para hospedar el equipamiento especificado en los servicios de aprovisionamiento.

5.2. ACEPTACIÓN DEL SERVICIO

La aceptación del servicio se dará cuando el **IMSS** valide por cada plataforma tecnológica lo siguiente:
Se dará por aceptado el servicio cuando todos los componentes y servicios que lo integran estén **instalados, configurados, puesta en marcha de la solución y validados por el personal asignado del IMSS**, de acuerdo a lo establecido en este anexo y se realice entrega de los documentos comprobatorios relacionados a cada servicio del presente anexo técnico, así como se cumpla con los entregables de única ocasión de acuerdo al ***plan de entrega*** establecido en conjunto con el **IMSS**. La validación de cada servicio será supervisada por personal que el **IMSS** designe.

5.3. LICENCIAMIENTO

La solución ofertada por el **LICITANTE** deberá considerar la totalidad de licencias de la solución integral para brindar todos los requerimientos establecidos en el presente anexo. La vigencia del licenciamiento para todos los servicios es necesaria desde su instalación durante la vigencia del contrato. En caso de que el **IMSS** requiera de licenciamiento adicional para el correcto funcionamiento de todos sus componentes este deberá ser proporcionado por el **LICITANTE** como parte del servicio.

5.4. PROCESOS

El **LICITANTE** deberá entregar toda la documentación que se genere durante la vigencia del contrato y deberá estar apegada a los formatos y procesos de **MAAGTIC-SI** o la normatividad vigente durante la ejecución del contrato. Los formatos que solicita el **IMSS** referentes al **MAAGTIC-SI** son los que actualmente están vigentes, sin embargo, al momento de la contratación y durante la vigencia del contrato dichos formatos solicitados en el presente anexo técnico podrán actualizarse, cancelarse, modificarse, sustituirse y/o en su caso incrementarse los formatos de acuerdo a los lineamientos que establezca la **Secretaría de la Función Pública** y la normatividad vigente.

5.5. RECURSOS HUMANOS

El **LICITANTE** deberá incluir los Recursos Humanos necesarios para la implantación y puesta en marcha de los servicios descritos en el presente anexo técnico, de acuerdo a los tiempos y niveles de servicio establecidos. El personal que realice funciones de coordinación, supervisión o cualquier otra función similar o superior que el **LICITANTE** proporcione, deberá tener el enfoque de atención a clientes, servicio y conocimiento técnico y operativo.

En caso de existir algún inconveniente con el personal, éste deberá ser reemplazado en caso de que el área lo solicite. Este cambio deberá realizarse en un plazo no mayor a 10 días hábiles.

Deberá contar con personal calificado y certificado de segundo y tercer nivel para atender los incidentes presentados en los servicios, para lo cual deberá trasladarse a las instalaciones del **IMSS** las veces que sea necesario.

Es importante señalar que en base a las necesidades de las Unidades Responsables del **IMSS**, esta lista podrá ser modificada de tal manera que puede solicitarse la rotación de personal o el movimiento temporal de los técnicos especialistas para atender eventos que así lo requieran.

El **LICITANTE** deberá considerar que el **IMSS** podrá requerir el apoyo de los ingenieros fuera de los días y horario mencionado para la atención del *Servicio* (Por eventos especiales, reubicaciones, servicios temporales, etc), por lo que este tipo de solicitudes deberán estar consideradas por el **LICITANTE**.

Deberá existir personal en un esquema 7x24, en caso de que el instituto requiera alguna eventualidad, se notificara para la coordinación respectiva con el **LICITANTE** por lo que deberán estar disponibles para la atención.

5.6. CLÁUSULA DE OPCIÓN PARA OBTENCIÓN DE BIENES AL CIERRE DE CONTRATO

El último mes de la prestación del servicio, el **IMSS** podrá evaluar quedarse con los bienes o conservar los bienes para lo cual informará al **LICITANTE** su decisión sobre la opción de compra de los bienes que integran el proyecto, el LICITANTE deberá presentar propuesta económica del o los componentes de hardware/software que integran cada uno de los servicios descritos en el presente anexo técnico, así como sujetarse al procedimiento que establezca el **IMSS** para formalizar este proceso.

Durante el último mes de la prestación del servicio, en caso de que el Instituto haya optado por la opción de compra, el **LICITANTE** realizará el proceso de entrega del equipamiento sujeto a la opción de compra por parte del Instituto. El **LICITANTE** deberá sujetarse al procedimiento que el **IMSS** requiera para formalizar este proceso.

6. ESPECIFICACIONES TÉCNICAS

Las especificaciones técnicas referentes a este apartado del anexo técnico se encuentran detalladas en el apartado **CARACTERÍSTICAS DE LOS SERVICIOS**.

7. PERFIL DEL LICITANTE

El **LICITANTE** deberá acreditar ser una empresa con la capacidad y experiencia técnica requerida para proporcionar el servicio solicitado, anexando currículo de la misma.

El **LICITANTE** deberá entregar al Instituto "La Opinión del Cumplimiento de Obligaciones en materia de Seguridad Social" vigente y positiva. Asimismo, el Licitante que resulte adjudicado queda obligado a entregar al Instituto junto con la factura de cobro respectiva, la "Opinión del Cumplimiento de Obligaciones en materia de Seguridad Social" vigente y positiva.

El **LICITANTE** deberá entregar el documento vigente expedido por el SAT en el que se emita la opinión de cumplimiento de las obligaciones fiscales, positivo y vigente.

El **LICITANTE** deberá contar con experiencia comprobable para brindar los servicios objeto del presente anexo técnico, apéndices, así como términos y condiciones.

ANEXOS
DIVISIÓN DE CONTRATOS

Certificaciones enunciativas más no limitativas en:

- ☐**CCIE Seguridad**
- ☐**CCIE Routing and Switching**
- ☐**CCIE Service Provider**
- ☐**CCNP Colaboración**
- ☐**CCDP Diseño Profesional de redes.**
- ☐**CCNA Cyber Ops**
- ☐**ITIL Foundation Certificate in IT Service Management**
- ☐**Symantec Data Loss Prevention Prevention 14.5**
- ☐**Symantec Messaging Gateway**
- ☐**APDS - Avaya Networking Solutions**
- ☐**APSS - Avaya Networking Solutions**
- ☐**ISO/IEC 27001**
- ☐**ISO/IEC 20000**
- ☐**ITIL intermediate in Service Design**
- ☐**ITIL intermediate in Operational support and analysis**
- ☐**ITIL intermediate in Service Offering AND Agreements**
- ☐**ITIL intermediate un Release, control and validación.**
- ☐**PCNSE Network Security Engineer 7**
- ☐**MCITP Enterprise Administrator on Windows Server 2008**
- ☐**MCTS Microsoft Exchange Server 2007 Configuration**
- ☐**Extreme Networks Design Specialist - Campus Fabric**
- ☐**Enterasys Certified Specialist – Routing**
- ☐**Enterasys Certified Specialist – Policy.**
- ☐**Security Competency – Technical Accreditation (SCT)**
- ☐**Network Automation Competency – Technical Accreditation (NCT)**
- ☐**Core Network Services Competency - Technical Accreditation (CNT)**
- ☐**Certificación ITIL RCV, 2017**
- ☐**Certificación ITIL SO, 2016**
- ☐**Certificación ITIL SOA, 2016**
- ☐**Certificación ITIL OSA, 2012**
- ☐**PMI**

El **LICITANTE** debe contar con el personal certificado en Metodologías de Administración de Proyectos para la dirección del proyecto.

El **LICITANTE** deberá presentar al Instituto, a través de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional cita en Av. Paseo de la Reforma No. 476, Anexo de Telecomunicaciones, Planta Alta, Col. Juárez, C.P. 06600, Ciudad de México, en un plazo no mayor a 5 (cinco) días hábiles posteriores a la adjudicación del contrato, al personal responsable del proyecto; en caso que no se presente el personal en el plazo marcado, se aplicará la pena correspondiente.

El **LICITANTE** deberá presentar en un plazo no mayor a 15 (quince) días hábiles posteriores a la adjudicación del contrato, un plan de trabajo general, para llevar a cabo la implementación del proyecto, en el que se especifiquen las actividades a realizar, la secuencia, los recursos asignados y responsables de dichas actividades, así como la duración del proyecto, su fecha de inicio y de conclusión marcando las fechas de entregables como son cantidad de servicios a entregar de forma única, mensual o eventual.

El **LICITANTE** deberá entregar en un plazo no mayor a 15 (quince) días hábiles posteriores a la adjudicación del contrato, una matriz de escalación con el personal que gestionará los servicios de TIC y con los que el Instituto estará colaborando, su cargo y puesto así como los datos y la vía de comunicación para contactarlo.

8. CONDICIONES TÉCNICAS DE ACEPTACIÓN DE ENTREGABLES

Normatividad

Los entregables deberán cumplir con los lineamientos y procesos que indica el **MAAGTIC-SI** o la normatividad vigente durante la ejecución del contrato.

Cumplimiento de obligaciones contractuales

Para la documentación de Cumplimiento de Obligaciones contractuales, que permita una fácil y organizada atención de procesos de auditoria por parte de los entes de fiscalización, el **LICITANTE** elaborará en un plazo no mayor a 15 (quince) días hábiles posteriores a la adjudicación del contrato, una matriz de los verbos, pronombres, tiempos y compromisos presentes en el anexo técnico, términos y condiciones, apéndices o documentación complementaria al anexo, así como en la propia oferta del **LICITANTE** ganador, a fin de contar con un listado de todos los verbos de acción, conjunciones, excepciones, interacciones, consideraciones de tipo y frecuencia de información electrónica que deba incluirse, casos de uso y en su caso especificaciones o excepciones, para convertirlos en los "documentos probatorios de cada obligación establecida en el contrato".

A partir de este listado, de manera conjunta entre el **IMSS** y el **LICITANTE**, en un plazo no mayor a 10 (diez) días hábiles posteriores a la entrega del listado por parte del Licitante que resulte adjudicado, generará el detalle de los documentos tanto en formato, contenido, información adjunta en imágenes, archivos o documentos complementarios, así como firmas y validaciones a efectuarse por el personal que participará en los procesos de entrega de servicios, lo cual se depositará en un repositorio documental que habilitará el **LICITANTE** con acceso permanente a los administradores del contrato (cuerpo de gobierno del contrato), los cuales analizarán al menos quincenalmente con el gerente de cuenta y personal técnico por parte del **LICITANTE**, el avance de los proyectos, la continuidad operativa, siguientes compromisos y la documentación del ejercicio del gasto y cumplimiento de niveles de servicio establecidos, siendo parte fundamental la documentación de Cumplimiento de Obligaciones contractuales, incluyendo en su caso, las penas convencionales o deductivas aplicables. En estas juntas de gobierno del contrato, el **LICITANTE** deberá exponer al personal **IMSS**, los detalles de la operación, consumos, tendencias, áreas de oportunidad y mejores prácticas susceptibles de incorporarse a la operación y administración del contrato, las cuales serán evaluadas por el **IMSS** y en su caso, autorizadas con o sin modificaciones, para su implementación y operación gradual o inmediata.
Para la exposición y análisis de la información presentada por el **LICITANTE**, éste deberá habilitar al menos 3 pantallas de al menos 75 pulgadas, con todo lo necesario para la presentación de información de la operación de los servicios tecnológicos que permitan exponer de manera gráfica y ágil lo descrito en los dos párrafos anteriores, lo que permitirá contar con información en línea constante de la operación de los servicios contratados incluyendo elementos de análisis y detalles de la operación (parámetros de utilización) de la infraestructura ofertada además de la prestación de los servicios, además de indicadores de negocio que puedan ser descritos desde el alcance de cada contrato.

Cláusulas y cumplimiento

a. Contrato de confidencialidad

El **LICITANTE** deberá firmar un Contrato de confidencialidad mediante el cual el **LICITANTE** se obliga a no revelar, transferir, compartir ni ceder ningún dato o información de carácter sensible y confidencial que se hayan compartido entre el **LICITANTE** y el **IMSS**.

b. Cláusula de Opción para Obtención de Bienes al cierre de contrato (entregable de infraestructura)

Durante el último mes de la prestación del servicio, en caso de que el Instituto haya optado por la opción de compra, el **LICITANTE** realizará el proceso de entrega del equipamiento sujeto a la opción de compra por parte del Instituto. El **LICITANTE** deberá sujetarse al procedimiento que el **IMSS** requiera para formalizar este proceso.

c. Documentación de cumplimiento de obligaciones

El **LICITANTE** con el objeto de fortalecer la supervisión y vigilancia de la administración del contrato materia del presente servicio y contribuir a las acciones para verificar la procedencia de los pagos, proporcionará un soporte especializado para la gestión del conocimiento administrativo relacionado con la prestación de los servicios de Nube **IMSS**.

Para que dicho conocimiento administrativo sea traducido en un activo del **IMSS**, el **LICITANTE** deberá aplicar el modelo de control de contratos definido por el Grupo de Gobierno del Contrato y ejecutará las acciones que se establecen en dicho modelo como un ejercicio permanente durante la vigencia del contrato. Para tal efecto, se deberá implementar un mecanismo para que dicho soporte especializado encargado de la gestión del conocimiento administrativo de los servicios objeto del presente anexo, cuente oportunamente con cada una de las solicitudes de servicio que se generen en el marco del contrato respectivo, así como respecto de todos los comunicados y documentos existentes entre el **IMSS** y el **LICITANTE** en relación con la prestación de los servicios. Lo anterior, toda vez que los servicios de soporte especializados previstos en ese aparatado están sujetos a flujo de información antes citada.

Lo anterior, con el fin de que el **LICITANTE** elabore los "Reportes de Administración" con corte mensual, que concluya las acciones relacionadas a la facturación presentada durante el periodo de la prestación del servicio, cuyo contenido se señala a continuación:

- **Gestión de los servicios**: Con base en las solicitudes u órdenes de servicio que genere el **IMSS**, el **LICITANTE** incluirá un desglose detallado del trámite que corresponde a la atención de cada una de ellas, en cuanto a su procedencia, tiempos límite de respuestas y demás circunstancias que se encuentren establecidas en el contrato respectivo y que permitan al Administrador del mismo tener control sobre dicha gestión, así como la documentación probatoria del devengo de los servicios, incluyendo toda la documentación o archivos electrónicos que demuestren la prestación del servicio, de conformidad a la funcionalidad solicitada y acorde a los niveles de servicio establecidos, siendo posible entre otros: reportes de monitoreo, disponibilidad, capacidad, desempeño y atención de incidentes, tickets de la mesa, actualizaciones, bitácoras, logs de aplicaciones, entre otros. En caso de que el licitante no cuenta con la documentación probatoria de los servicios devengados, estos no podrán ser facturados.

- **Plataforma de obligaciones:** En este apartado, el **LICITANTE** elaborará un listado que identifique la totalidad de las obligaciones que se encuentran plasmadas en el contrato y sus respectivos anexos relacionados con los servicios. Asimismo, llevará a cabo su clasificación en atención a su importancia y consecuencia en:

  a. Obligaciones principales. Condicionantes del pago y los que están asociados a penas y deductivas
  b. Obligaciones secundarias. No condicionan el pago de los servicios, sin embargo, su cumplimiento es obligatorio en términos del instrumento contractual.

  El **LICITANTE** deberá presentar la documentación descrita en el presente punto, previo a solicitar el pago de sus servicios.

Asimismo, el **LICITANTE** proporcionará la representación gráfica y analítica de una línea de tiempo en el cual se detallen las fechas límite para el cumplimiento de obligaciones primarias y secundarias conforme a las órdenes de servicio y los plazos y procedimientos previstos en el contrato respectivo.

- **Análisis de consecuencias:** El **LICITANTE** realizará un análisis respecto de la aplicación del sistema de sanciones previsto en el contrato durante la vigencia del mismo, con base en las solicitudes u órdenes de servicio recibidas y la atención dada a las mimas. Con esta información el Administrador del Contrato efectuará las acciones de verificación que permitan la aplicación de las reglas de proporcionalidad establecidas en los numerales referentes a penas convencionales y deductivas por prestación deficiente del servicio y su cumplimiento normativo, así como el cálculo de las sanciones que resulten aplicables conforme a lo establecido en el Instrumento Contractual y la normatividad vigente; en este sentido, los reportes de administración deberán incluir dichos elementos.

- **Control presupuestario:** El **LICITANTE** con base en las solicitudes de servicio que se presenten durante la vigencia del contrato respectivo y la atención brindada a las mismas, incluyendo las cancelaciones correspondientes, realizará un informe analítico del importe de los servicios devengados que incluya un desglose por cada tipo de servicio en relación con los montos y máximos establecidos en dicho instrumento jurídico; lo anterior, a efecto de facilitar las actividades de verificación de los consumos presentados y tener un control presupuestario de los mismos. En este componente se incluirán también aquellos documentos impresos o electrónicos que incidan en este rubro tales como: tendencias en el consumo financiero, ejercicio presupuestal por dirección normativa, por aplicativo y por tipo de tecnología, esto es detallado por centro de costos, servicios devengados, control de saldos presupuestales (pasivos) y proyecciones presupuestales, entre otros.

- **Aspectos técnicos y metodológicos de los entregables:** El **LICITANTE** identificará y relacionará los elementos especificados en el contrato y sus anexos conforme a los cuales deberán presentarse los servicios considerando los entregables pactados, desde una perspectiva técnica y metodológica. Conforme a lo anterior, se incluirá en los reportes un informe que contenga los elementos exigidos en el contrato y sus anexos, con los cuales deberá acreditarse la entrega o prestación de los servicios. Identificando, entre otros elementos: (i) forma; (ii) plazos, (iii) servidores públicos responsables de la recepción, sus cargos y ubicaciones; (iv) lugares de entrega o prestación de servicios; (v) procedimiento para la suscripción de las actas; (vi) documentación de soporte solicitada que acredite fehacientemente la entrega de los servicios devengados de conformidad con la funcionalidad solicitada así como los niveles de servicio establecidos, y en su caso la propuesta de la posible aplicación de penas convencionales y deductivas, entre otros elementos.

ANEXOS
DIRECCIÓN DE CONTRATOS

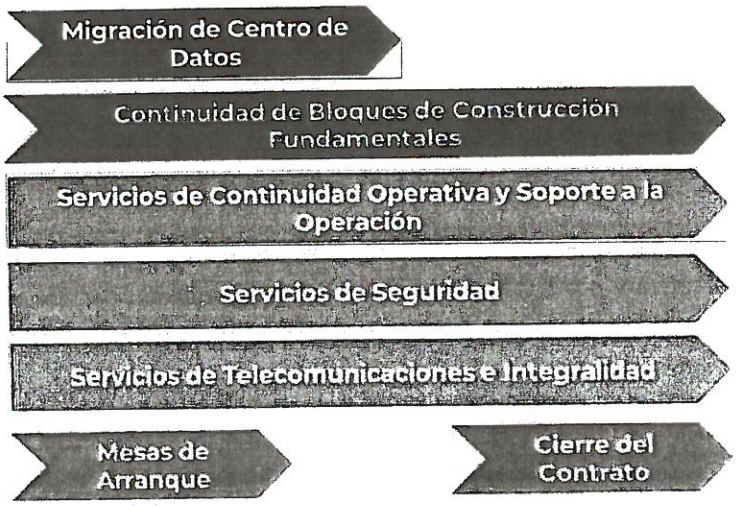
- **Esquema de integración de pagos:** El **LICITANTE** incluirá en los reportes la identificación de los elementos justificativos y comprobatorios que soporten la prestación de servicios durante el periodo que se reporte, conforme a las disposiciones normativas vigentes. Con esta información, el **LICITANTE** integrará la carpeta que soporte la solicitud de pago ante el **IMSS** por la entrega o prestación de los servicios devengados en el periodo mensual correspondiente, para su trámite y gestión por parte del Administrador del contrato, en términos de las facultades con que cuenta para la aceptación de los servicios.

- **Proyección del consumo de los servicios**: Con base en las facturas identificadas para pago, el **LICITANTE** elaborará un modelo gráfico y analítico que registre el consumo mensual real de cada uno de los servicios facturados y que permita un análisis comparativo respecto al consumo programado, a efecto de brindar al administrador del contrato información para la toma de decisiones. Los reportes de administración para la gestión del conocimiento administrativo de los servicios deberán formar parte invariablemente de los documentos justificativos que soportan cualquier pago que se realice durante la vigencia del contrato correspondiente.

9. CRONOGRAMA DE ACTIVIDADES

El Plan de Trabajo General especifica las fases más relevantes del contrato, el **LICITANTE** deberá entregar el plan de trabajo y establecer los tiempos máximos que prevé emplear en cada una de ellas a fin de dar cumplimiento de las obligaciones relacionadas a los servicios del presente anexo técnico.

Servicio de Continuidad de la Nube 2020



Marco de referencia del Plan de Trabajo General

El **LICITANTE** en su propuesta deberá incluir el Plan de Trabajo General, que deberá especificar hitos y fases para el cumplimiento de los servicios del presente anexo técnico, mismos que serán respetados en todo momento tanto en fechas y compromisos establecidos como en el alcance y funcionalidad ofertada. El **LICITANTE** deberá de integrar en su propuesta, las definiciones o peticiones de servicio que se establecen en este Anexo Técnico y que son vinculadas a una o más fases del Plan de Trabajo General.

A continuación se especifica de manera enunciativa más no limitativa, una tabla-resumen de los hitos que se prevén en el Plan de Trabajo General para los servicios descritos en el presente anexo técnico, indicando Fase, Identificador del hito en cuestión (ID), el nombre o descripción del hito, las fechas relativas y absolutas de inicio y/o término, cantidad de días naturales máximos de duración por hito que el posible **LICITANTE** oferte.

Tabla Hitos relevantes a considerar en el Plan de trabajo

Fase	ID	Hito	Inicio / Término Relativo de Hito	Máxima duración en días naturales	Precedente(s)
Proceso de Migración de Centro de Datos actual al Servicio de Continuidad de Nube IMSS 2020.					
Planeación del Arranque	1	Kick-Off y presentación del equipo de trabajo del LICITANTE.	A más tardar 10 días naturales posteriores al Fallo	Plazo ofertado por el posible LICITANTE	N/A
	2	Mesas (sesiones) de trabajo de Planeación del Arranque, entre el LICITANTE y el IMSS, convocadas por el Grupo Administrador del Contrato IMSS	Plazo ofertado por el posible LICITANTE	Plazo ofertado por el posible LICITANTE	1
	3	Presentación, por parte del LICITANTE del Plan de Trabajo Detallado	A más tardar 5 días naturales posteriores a la finalización de las Mesas de Trabajo	Plazo ofertado por el posible LICITANTE	2

	4	Análisis y Revisión (en su caso aprobación) del Plan de Trabajo Detallado de parte del Grupo Administrador del Contrato del IMSS	A más tardar 15 días naturales posteriores a la entrega del Plan Detallado de parte del LICITANTE	Plazo ofertado por el posible LICITANTE	3
	5	En caso de aplicar, incluir firma de Acuerdos de Nivel de Operación (OLAs) entre el **LICITANTE** y Terceros Involucrados en los servicios del presente anexo técnico.	A lo largo de los siguientes 25 días naturales a partir del Kick-Off del proyecto	Plazo ofertado por el posible LICITANTE	1
Actividades de migración de centro de datos actual y continuidad de la operación de servicios.	6	Inicio de actividades de migración del centro de datos actual al centro de datos del **LICITANTE** incluyendo servicios de punto neutro.	Al día natural siguiente a la aprobación, por parte del IMSS, del Plan de Trabajo Detallado	Plazo ofertado por el posible LICITANTE	4
	7	Finalización de actividades de migración del centro de datos actual al centro de datos del **LICITANTE** incluyendo punto neutro.	Plazo ofertado por el posible LICITANTE	Plazo ofertado por el posible LICITANTE	4
	8	Estabilización de los Niveles de Servicio a la finalización de la	Plazo ofertado por el posible LICITANTE	Plazo ofertado por el posible	6 y 7

		etapa de migración.		LICITANTE	
	9	Inicio de los Servicios asociados a la continuidad operativa de los servicios del presente anexo técnico.	Plazo ofertado por el posible LICITANTE	Plazo ofertado por el posible LICITANTE	N/A
	10	Actividades de Finalización del Contrato.	A más tardar 4 meses naturales antes del día de la Finalización del Contrato	31 de diciembre de 2020	N/A
CIERRE	12	Finalización del Contrato	-	31 de diciembre de 2020	N/A

El **LICITANTE** deberá elaborar Programas de Trabajo Detallados que sean necesarios para la puesta a punto de cada uno de los servicios de:

- Servicio de Continuidad y Gestión de la Operación
- Servicio de Operación y Calidad de la Seguridad informática perimetral
- Servicio de integralidad de ambientes distribuidos a nivel nacional y telecomunicaciones
- Servicio de Gestión de Medición del Desempeño de Aplicativos y Componentes Institucionales

10. NIVELES DE SERVICIO

El proceso de Administración del Nivel del Servicio deberá involucrar tanto al **LICITANTE** como al **IMSS** para mantener y monitorear el adecuado funcionamiento del servicio. El **LICITANTE** deberá mantener una revisión continúa de los logros de servicio para garantizar que la calidad del servicio sea mantenida y mejorada permanentemente.

Nivel general de servicio

Los niveles de servicio establecidos que deberá cumplir el licitante en la prestación de los servicios es el siguiente:

El nivel de servicio base para este contrato es de:

Nivel de Disponibilidad	Minutos indisponibles permitidos en el mes para los servicios del presente contrato
99.982% sobre la plataforma instalada (TIER III)	7.8 minutos

Esta disponibilidad establecida incluye el servicio de soporte técnico en caso de falla en un esquema de 7x24 en días y horarios hábiles con soporte presencial certificado, por lo que en su caso, será exigible la participación de especialistas únicamente en estos horarios, sin embargo, puede requerirse presencia en un esquema 7x24 del personal asociado al servicio, a petición del Instituto.

10.1. Categorías de Niveles de Servicio

Con el fin de lograr una administración más ágil se han clasificado los acuerdos de nivel de servicio en dos categorías:

La primera categoría hace referencia a los **niveles de servicio de gestión**, los cuales miden la calidad de la entrega y gestión de cada uno de los servicios del Anexo Técnico.

La segunda categoría está relacionada con los **niveles de servicio de infraestructura**, los cuales medirán la calidad de la disponibilidad y el desempeño de los componentes que integran los servicios del Anexo técnico.

El Instituto y el **LICITANTE** podrán generar métricas adicionales, que junto con las anteriores, las cuales servirán para medir el servicio proporcionado.

El posible **LICITANTE** incluirá en su propuesta técnica, la solución automatizada de medición de los diferentes niveles de servicio antes de su implementación, estableciendo claramente los elementos involucrados en el aprovisionamiento del servicio, las formas de medición, el método de tratamiento de la información generada para su consolidación, los reportes, estadísticas, documentación que deberá ser entregada, intervalos de medición y la forma como se harán disponibles los resultados al Grupo de Gobierno de Contrato para su dictamen consolidado.

El **LICITANTE** utilizará las herramientas habilitadas en el **Servicio de Continuidad Operativa y Soporte** como entrada de datos, así como herramientas utilizadas por el Instituto (BMC Remedy y/o cualquier otra que indique el Instituto) mismas que deberán ser definidas en las mesas de arranque de contrato; así como

proveer, instalar y habilitar la Infraestructura y el licenciamiento de su propia herramienta, incluyendo los elementos de hardware y software necesarios para el acopio, consolidación, explotación de información y generación de reportes e informes.

La herramienta del **LICITANTE** estará accesible desde cualquier punto de la red del Instituto, con la finalidad de mostrar de forma clara y oportuna la información que soporta el nivel de servicio ofrecido, teniendo la posibilidad de contar con indicadores globales y consolidados dependiendo del tipo de métrica y también de observar el detalle que compone estos indicadores. Dicha infraestructura de hardware y software estará sujeta a los niveles de servicio descritos en el presente documento.

El **LICITANTE** proporcionará la transferencia de conocimiento y entrenamiento tecnológico necesario en el manejo y administración de las herramientas de niveles de servicio para al menos 20 personas, en las instalaciones que se acuerden con el Instituto. El calendario y fechas de la transferencia de conocimiento y entrenamiento tecnológico se impartirán durante las fechas acordadas en las mesas de arranque del servicio.

El software propuesto para niveles de servicio deberá cumplir al menos con los siguientes aspectos, mencionados de manera enunciativa más no limitativa:

- Acceso a las herramientas desde la red del Instituto e Internet
- Generación de reportes (Excel, RTF, PDF, etc.)
- Generación de Estadísticos (gráficas, dashboard)
- Medir los tiempos de atención
- Que se pueda importar y exportar información
- Consulta de información en tiempo real
- Contenga pistas de auditoría de cada evento
- Se pueda migrar de plataforma
- Contemple notificaciones electrónicas
- Ambiente gráfico
- Multiusuario
- Mantenimiento de respaldos
- Disponibilidad
- Repositorio de los reportes (digitalizados) a entregar durante el contrato

10.2. Definición General de Entrega

La entrega de los servicios administrados, como los descritos en el presente Anexo Técnico, se define como el evento de cumplimiento en la entrega del servicio ofrecido al Instituto por el **LICITANTE**.

Un evento será considerado como realizado satisfactoriamente cuando el Instituto, a través del personal y/o las áreas correspondientes, proporcionen retroalimentación o confirmación aprobatoria para su cierre. El **LICITANTE** y el Grupo de Gobierno del Contrato precisarán de manera formal en mesas de arranque, las políticas y evidencias de aceptación para cada tipo de entrega, los cuales podrán ser actualizados conforme a las necesidades del Instituto.

Se entiende por acción solicitada a cualquier evento, requerimiento, solicitud registrada y/o notificada de manera formal y oportuna por el Instituto hacia el **LICITANTE**, conforme al procedimiento y las herramientas establecidas para tal fin (Mesa de Servicio del **LICITANTE** o Instituto, o cualquier otra definida en las mesas de arranque).

Dentro de la Entrega del Servicio, se incluye la atención de diferentes requerimientos, solicitudes, eventos, o situaciones que comprenderán varios tipos de esquemas de atención, a describirse dentro de cada sección especifica, dedicada a los diferentes servicios del presente anexo técnico.

10.3. Reportes del Servicio

Con el objeto de medir la entrega, disponibilidad y desempeño de los servicios proporcionados, el **LICITANTE** definirá y generará los reportes de niveles de servicio de los servicios solicitados, que serán parte de los entregables periódicos del servicio.

Los reportes deberán ser generados con base en las herramientas habilitadas para tal efecto (en los casos que aplique) y ser entregados por el **LICITANTE** al Grupo de Gobierno del Contrato de la siguiente manera:

Num.	Nombre y Descripción	Frecuencia del reporte	Inicio de la Entrega
01	Reporte de nivel de servicio: **Entrega del Servicio** desglosado por tipo de servicio	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
02	Reporte de nivel de servicio: **Disponibilidad** desglosado por tipo de servicio	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
03	Reporte de nivel de servicio: **Desempeño** desglosado por tipo de servicio	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
04	Reporte de nivel de servicio: **Impacto a la operación**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
05	Reporte de nivel de servicio: Atención de Solicitudes en la Operación del Servicio.	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio

	06	Reportes de Administración por Procesos: Incidentes y Problemas a) El **LICITANTE** debe entregar al Grupo de Gobierno del contrato reporte de análisis de cumplimiento de los tiempos de solución de incidentes. b) Para los incidentes de que dejen la operación detenida o parcialmente detenida, el **LICITANTE** deberá entregar reporte técnico y ejecutivo. c) Por excepción el Instituto podrá solicitar los reportes anteriormente indicados para los incidentes de prioridad 3 (operación parcialmente detenida en un proceso de negocio).	a) Se entregarán dentro de los primeros 05 días hábiles de cada mes. b) Se entregarán 3 días hábiles después de haber concluido la atención del mismo. c) Se entregarán 5 hábiles después de haber concluido la atención del mismo.	Una vez iniciado el servicio	
	07	Reportes de Administración por Procesos: Administración de configuraciones. El **LICITANTE** debe entregar un reporte en donde se identifiquen las configuraciones y cambios que se hayan realizado a la infraestructura (actualización de la memoria técnica de los servicios).	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio	
	08	Reportes de Administración por Procesos: Administración de Cambios El **LICITANTE** debe entregar un reporte en donde se	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio	

	identifiquen los cambios (RFCs) ejecutados. .		
09	Reportes de Administración por Procesos: Administración de Problemas El **LICITANTE** debe entregar un reporte en donde se identifiquen los problemas identificados.	Se entregarán dentro de los primeros 10 días hábiles de cada mes devengado	Una vez iniciado el servicio
10	Reportes de utilización y desempeño. Deberá contener estadísticas principales de uso y desempeño, así como las tendencias de todos los componentes del servicio. Se acordará en la Planeación del Arranque el contenido de este tipo de reportes.	Se entregarán dentro de los primeros 10 días hábiles de cada mes vencido	Una vez iniciado el servicio
11	Reportes, informes o entregables descritos en las secciones de cada servicio	Se entregaran acorde a lo especificado en el apartado o en los tiempos definidos en las mesas de arranque.	Una vez iniciado el servicio

Tabla Reportes de Niveles de Servicio

El detalle de los atributos, variables y formato de los reportes requeridos en este apartado y en general en los descritos en los apartados del presente anexo técnico, serán propuestos por el **LICITANTE** para la aprobación del Instituto durante las mesas de arranque. El Instituto podrá acordar con el **LICITANTE** modificaciones a los mismos.

Los reportes, entregables, productos de trabajo mencionados en este apartado y en general en los apartados descritos en los servicios del presente anexo técnico, deberán ser atendidos por el **LICITANTE** bajo los siguientes lineamientos que se mencionan de manera enunciativa más no limitativa:

- Deberán entregarse con la periodicidad establecida en el presente anexo técnico, apéndices o en las mesas de trabajo.

- El Instituto podrá solicitar en cualquier momento, una copia en medio electrónico del contenido total o parcial de la información, misma que será entregada a más tardar 07 días hábiles después de su solicitud.

Consideraciones generales para los reportes de nivel de servicio

Disponibilidad

Reportes de cumplimiento de acuerdos de niveles de servicio establecidos para cada uno de los servicios del presente anexo técnico.

Reportes con diagramas, tablas e histogramas de distribución y sumarización del comportamiento global del servicio para los parámetros definidos en periodos de tiempo determinados por el Instituto.

Los reportes de niveles de servicio tendrán de manera enunciativa más no limitativa las siguientes características:

- Identificación del recurso
- Mes que se evalúa
- Valores esperados en el mes para cada Nivel de Servicio medido
- Valores obtenidos en el mes para cada Nivel de Servicio medido
- Diferencia entre el Valor esperado y el Valor obtenido
- Total del monto a penalizar en el mes

Entrega del servicio

Reportes de cumplimiento de acuerdos de niveles de servicio establecidos para cada una de las acciones concluidas en el mes bajo evaluación.

Reportes con diagramas, tablas e histogramas de distribución y sumarización del comportamiento global del servicio para los parámetros definidos anteriormente en periodos de tiempo determinados.

Los reportes de niveles de servicio tendrán las siguientes características mínimas:

- Mes que se evalúa
- Cantidad total de acciones realizadas en el mes
- Cantidad total de acciones realizadas dentro de la ventana de tiempo establecida en el mes
- Anexo de relación de acciones realizadas, identificando su tipo, tiempo de inicio y finalización
- Valores esperados en el mes para cada Nivel de Servicio medido
- Valores obtenidos en el mes para cada Nivel de Servicio medido
- Diferencia entre el Valor esperado y el Valor obtenido
- Total del monto a penalizar en el mes.

10.4. Objetivos y Métricas específicas de Niveles de Servicio

En el Apéndice denominado **"Objetivos y Métricas de Niveles de Servicio"** se describen con detalle las métricas, objetivos y los mecanismos y/o procedimientos de cálculo de los niveles de servicio para cada uno de los servicios descritos en el presente Anexo Técnico.

11. DESCRIPCIÓN GENERAL DE ENTREGABLES

El Instituto requiere recibir distintos tipos de documentos o reportes, que favorezcan el desempeño y la continuidad del servicio, para que acrediten y de certidumbre a las actividades diarias que el **LICITANTE** efectuará bajo la supervisión del Instituto para tales efectos. Estos documentos no deben ser confundidos con aquellos que integran la Propuesta Técnica de los posibles **LICITANTES** en el proceso de contratación, mismos que se describen con detalle en el apartado correspondiente de la convocatoria objeto del presente Anexo Técnico.

Para una mejor identificación, los entregables que el **LICITANTE** elaborará a lo largo de la vigencia del contrato, se dividen en aquellos que se efectúan "por única vez" y aquellos que se elaboran de manera periódica (mensual o bajo demanda).

Es importante destacar que la totalidad de los entregables que el **LICITANTE** efectúe, de acuerdo con las disposiciones descritas en el presente Anexo Técnico, estarán alineados a la normatividad vigente aplicable en el Instituto (MAAGTIC-SI). El Instituto podrá entregar al **LICITANTE**, los formatos que a este respecto tenga en su poder para la elaboración de los documentos y reportes relacionados con los entregables, durante las Mesas de Trabajo de del Arranque del servicio.

El **LICITANTE** se compromete a entregar, de manera formal a lo largo de la vigencia del contrato, un conjunto de documentos relacionados a cada servicio requerido en el presente anexo técnico.

Cualquier entregable adicional a los listados a continuación y que no se encuentre en la descripción de los servicios del presente anexo técnico, y que el **LICITANTE** considere necesario para establecer para una relación más eficiente entre el **LICITANTE** y el Grupo de Gobierno de Contrato, será propuesto por el **LICITANTE**, revisado y en su aceptado por el GGC para optimizar el desempeño del servicio en su conjunto.

A continuación se listan los entregables asociados a los servicios que requieren una especificación puntual, sin menos cabo de todos los entregables, productos de trabajo y cualquier obligación descrita en los servicios objeto del presente anexo técnico.

11.1. Entregables asociados a los Servicio de Continuidad de la Operación y Soporte

ID	Nombre del Entregable	Descripción	Modalidad	Compromiso de Entrega
1	Criterios de aceptación de los entregables asociados a la puesta en marcha y operación de los Servicios. Este entregable tendrá como alcance el formato estandarizado de todos los documentos que se entregan.	Documento que enumera los Criterios de Aceptación acordados durante el Arranque del Servicio, con los elementos propuestos	Única Vez	15 días después del arranque del servicio

		por el LICITANTE para que el IMSS pueda avalar la entrega-recepción de los servicios prestados		
2	Plan de Mantenimientos Preventivos (Road Map) de las plataformas de cómputo y/o procesamiento.	Road Map anual de Mantenimientos Preventivos para garantizar la correcta operación de la infraestructura	Única Vez	30 días después del arranque del servicio
3	Categorizaciones para Mesa de Servicio del **LICITANTE**	Documento con la categorización de solicitudes de cambios, incidentes y problemas durante la operación de los Servicios para garantizar la correcta implementación de su mesa de servicio.	Única Vez	30 días después del arranque del servicio
4	Proceso de Gestión de incidentes	Descripción del proceso que se llevará a cabo para la Gestión de Incidentes	Única Vez	30 días después del arranque del servicio
5	Proceso de Gestión de problemas	Descripción del proceso que se llevará a cabo para la Gestión de Problemas	Única Vez	30 días después del arranque del servicio
6	Proceso de Gestión de cambios	Descripción del proceso que se llevará a cabo para la Gestión de Cambios	Única Vez	30 días después del arranque del servicio

ANEXOS
DIRECCIÓN DE CONTRATOS

7	Inventario con el estado Actual de los Servicios	El **LICITANTE** deberá identificar nuevamente y actualizar la matriz de Servicios Críticos.	Única Vez	Semestral
8	Monitoreo de Niveles del Servicio de Disponibilidad de la Infraestructura	Herramienta que permita monitorear los niveles de servicio de la infraestructura crítica para la Operación de los Servicios del IMSS	En línea	60 días después del arranque del servicio
9	Reporte de Gestión de Requerimientos	Documento que contiene la volumetría mensual de las solicitudes (tickets) registrados en la herramienta de la mesa de servicio del LICITANTE que se registran para la atención del instituto	Mensual	1 mes
10	Reporte de Gestión de Incidentes	Documento que contiene la volumetría de los incidentes presentados durante el mes	Mensual	1 mes
11	Documento con los casos de soporte solicitados hacia el fabricante del producto	Documento con el listado de casos reportados con los respectivos fabricantes de las soluciones tecnológicas, indicando el estado que guarda cada uno	Mensual	1 mes
12	Reporte Mensual de Activos para la Operación del Servicio	Reporte con el inventario de los activos que forman parte del ecosistema tecnológico utilizado para	Mensual	1 mes

		la entrega de los servicios		
13	Reporte de Gestión de Eventos	Documento que contiene la volumetría de los eventos presentados durante el mes, agrupándolos los que tuvieron impacto.	Mensual	1 mes
14	Reporte de Gestión de Problemas	Documento que continúen la volumetría de los problemas registrados durante el mes.	Mensual	1 mes
15	Reporte de Gestión de Cambios.	Documento que continúen la volumetría de los cambios registrados durante el mes, así como su calendario y las afectaciones a los activos en la CMDB	Mensual	1 mes
16	Reporte de tickets generados	Documento que continúen la volumetría de los ticket's generados durante el mes	Mensual	1 mes
17	Informe de la implementación de actualizaciones de las versiones del Sistema Operativo. Base de Datos, Middleware, componentes y/o Subsistemas	Documento que contiene evidencia de las actualizaciones de versionamiento del software	Mensual	1 mes

18	Reporte de los certificados que caducan	Informe de caducidad o vigencia de los certificados de seguridad instalados en los ambientes soportados. (por evento, 90 días naturales antes del vencimiento).	Mensual	1 mes
19	Informe Mensual del Servicio (Informe de las versiones de Sistema Operativo).	Documento que continúen las versiones del sistema operativo	Mensual	1 mes
20	Documento con evidencia de la herramienta tecnológica para la visibilidad de los servicios	Un documento que muestre las funcionalidades y alcances de la herramienta	Mensual	1 mes
21	Reporte de Gestión de Configuraciones	Documento con los modelados de la CMDB	Mensual	1 mes
22	Reporte de Incidente (Post-Mortem)	Documento que continúen la cronología o en algunos casos la causa raíz que provoco un incidente relevante (Mayor)	Bajo Demanda	72 horas
23	Servicios cotizados eventualmente	Informe por evento de servicios consumidos del catálogo de Servicios.	Bajo Demanda	1 mes
24	Reporte Dictamen Técnico	Documento que continúen el dictamen técnico al cierre del problema	Bajo Demanda	1 mes

25	Plan de Trabajo del Tuning en todos los ambientes que aplique al mes vencido que se ejecutó	Plan de trabajo que se ejecutó para la afinación de configuración de servicios	Bajo Demanda	1 mes
26	Plan para Integrar resultados y avances de la consolidación/migración tecnológica en el mes que se realice	Plan de trabajo ejecutado en una consolidación física	Bajo Demanda	1 mes

12. CATALOGOS DE SERVICIOS

El Catálogo de Servicios del presente Anexo Técnico resume los elementos de servicio que son considerados elementos de pago en el contrato correspondiente, y todos ellos guardan relación con servicios descritos en uno o varios apartados de este Anexo Técnico. Los costos de los servicios solicitados en este Anexo Técnico serán pagados por el IMSS a mes vencido, independientemente de si se refieran a servicios bajo un régimen "Unitario Mensual" o a servicios bajo un esquema "Por Evento" (en cuyo caso será liquidado totalmente).

12.1. Servicios Agregados (Recurrentes)

1	Infraestructura y Bloques de Construcción Fundamentales	Unitario Mensual	Servicios para el aprovisionamiento, implementación, operación y soporte de Bloques de Construcción Fundamentales y Comunes.
2	Infraestructura y Bloques de Construcción Comunes	Unitario Mensual	Servicios para el aprovisionamiento, implementación, operación y soporte de plataformas de virtualización o extensión de nube que permitan la

			integración y el despliegue de determinados BCF según se señalan en el Apéndice "Bloques de Construcción Fundamentales" y los BCC que se definan a partir de los mismos.
	Punto Neutro	Unitario Mensual	Servicios para innovar la forma de interconexión entre distintos Proveedores de enlaces digital mediante una infraestructura multiplataforma y multicarrier, en donde distintos Proveedores de servicio de conectividad interactúan de manera transparente, otorgando así, el intercambio ágil y oportuno de la información necesaria entre las unidades Médico Administrativas del Instituto.
	Servicio de Continuidad Operativa y Soporte	Unitario Mensual	Servicios para la gestión, ejecución, mantenimiento, soporte y aseguramiento del aprovisionamiento de los servicios del Instituto dentro de los niveles de servicio acordados.
Servicios de Seguridad			
	Servicio de Administración y Soporte de Componentes de Seguridad	Unitario Mensual	Servicios para aprovisionar, administrar y soportar componentes de hardware de seguridad para proteger la infraestructura informática y la información contenida en dicha infraestructura.

	Centro de Operaciones de Seguridad (SOC)	Unitario Mensual	Servicios para gestionar un Centro de Operaciones de Seguridad (SOC) cuyo objetivo es operar y soportar la infraestructura de seguridad y los servicios asociados para proteger los activos de información contenida en dicha infraestructura.
	Servicio de Control de Calidad de la Seguridad	Unitario Mensual	Servicios para gestionar y ejecutar controles de calidad de seguridad para dar certeza de las configuraciones o servicios para proteger la información contenida en la infraestructura informática la cual puede ser proporcionada por un tercero.

12.2. *Servicios Desagregados (Por evento)*

	Tipo de Servicio		
	Unidades de Soporte Extendido	Mediante USEs	Servicios para la ejecución de proyectos o servicios que por su naturaleza tienen una demanda de recursos y esfuerzos variables por lo que su alcance y estimación de recursos son acordados previos a su ejecución.

ANEXOS
DIVISIÓN DE CONTRATOS

13. PROCESO DE ENTREGA AL TÉRMINO DEL CONTRATO

Una vez concluida la prestación del servicio, el **LICITANTE,** entre otras cosas, realizará el proceso de entrega de todo el equipamiento, software, configuración, desarrollos, CMDB, base de datos de conocimiento, diagramas, bases de conocimiento de configuración de: hipervisores, contenedores, sistemas operativos huésped, software especializado, sistemas, aplicativos, servicios, bases de datos, web services, servidores de aplicación, balanceadores, monitoreo y en general de todas las herramientas y funcionalidades de todo lo que haya sido incorporado como parte del proyecto o en su caso, producto del servicio, incluyendo cualquier componente de hardware/software que integre dicho servicio descrito en el presente documento, así como en la propuesta del Licitante. El **LICITANTE** deberá sujetarse al procedimiento que el **IMSS** requiera para formalizar este proceso.

14. RELACION DE APENDICES

Apéndice 1 Bloque de Construcción Fundamentales
Apéndice 2 Ubicaciones Geográficas
Apéndice 3 Esfuerzos realizados para la migración de centro de datos actual
Apéndice 4 Relación actual de Infraestructura en Centro de Datos y proyección de crecimiento
Apéndice 5 Especificaciones técnicas de seguridad de la información
Apéndice 6 Objetivos y Métricas de Niveles de Servicio
Apéndice 7 Glosario

15. FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN

Responsables de Elaboración

Héctor Martínez Valenzuela
Titular de la División de Telecomunicaciones
12/11/2019

Alejandro Paniagua Ramírez
Titular de la División de Administración de Riesgos Tecnológicos
12/11/2019

Carlos Francisco Ramírez del Rivero,
Titular de la División de Administración y Continuidad de la Operación
12/11/2019

Héctor Javier Reyes Oropeza
Titular de la División de Administración, Procesamiento y Almacenamiento
12/11/2019

Responsables de Revisión

Javier Cortés López
Titular de la Coordinación Técnica de Operación de Servicios Tecnológicos
12/11/2019

ANEXOS
DIVISIÓN DE CONTRATOS

Carlos Calderón Zacarias
Titular de la Coordinación Técnica
de Redes y Telecomunicaciones
12/11/2019

Responsables de Aprobación

Eduardo Oropeza Ortiz
Titular de la Coordinación de
Sistemas de Infraestructura
Tecnológica Institucional
12/11/2019

Servicios de Continuidad de la Nube IMSS 2020

Apéndice #1. Bloques de Construcción Fundamentales

Contenido

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	14/10/2019	Elaboración de documento	Ing. Héctor Javier Reyes Oropeza Lic. Carlos Francisco Ramírez del Rivero Ing. Héctor Martínez Valenzuela Ing. Alejandro Paniagua Ramírez
0.2	28/10/2019	Actualización del documento	Ing. Javier Cortés López Ing. Carlos Calderón Zacarías
1.0	12/11/2019	Aprobación del documento	Ing. Eduardo Oropeza Ortiz

1. Objetivo del documento

El objetivo del presente Apéndice es establecer la descripción de los Bloques de Construcción Fundamentales referidos en el Anexo Técnico del Servicio Administrado objeto de esta Licitación.

2. Infraestructura

2.1. Plataforma

2.1.1. Hardware

Servidores de medio desempeño

2.1.1.1.1. Servidor RISC Modalidades M1, M2 y M6

El procesador deberá tener al menos alguna de las siguientes arquitecturas BASE:

- Oracle SPARC T5-8 Server
  - SPARC T5 16-cores a 3.6 GHz
  - 128 threads por procesador
  - Cache 8 MB compartidos, Level 3 Cache; 128 KB Level 2
- IBM Power Systems Enterprise Servers
  - 24 to 48 cores (12-core) a 3.72 GHz
- HP Integrity Servers
  - 16 processors/240 cores a 2.8 GHz
  -

Y deberá ser escalable con al menos incrementos de:

- Módulos de 2 Procesadores con 128 threads

La memora RAM BASE deberá ser cuando menos de:

- 1TB de memoria RAM

Y deberá tener incrementos de cuando menos:

- 1 TB de memoria RAM

El HBA deberá tener al menos 4 tarjetas y/o HBAs:

- 2 para soporte a la SAN velocidad mínima 10 Gbps (FC, ISCSI o FCoE)
- 2 para respaldo velocidad mínima 10 Gbps Ethernet

La Interface de video deberá estar Integrada a la tarjeta madre

La Interface de red deberá incluir por lo menos:
- 8 puertos de red RJ45, velocidad 10 Gbps Ethernet.

El equipo deberá contar al menos con 2 fuentes internas de poder hot plug redundantes.

El equipo deberá contar al menos con 2 ventiladores internos.

El equipo deberá tener las siguientes características RAS:
- Discos Hot-plug
- Tarjetas PCIe Hot-plug
- Fuentes de Alimentación y Ventiladores redundantes hot-swap
- Comprobación y Corrección de errores y paridad de memoria
- Fácil sustitución de componentes
- Controladores de disco RAID 0, 1 y 1E / 10 integrado
- Arquitectura de gestión de averías incluyendo Predictive Self Healing

Para la Administración remota el equipo deberá contar con tarjeta de administración remota que permita la administración del mismo en una interfaz de modo texto, incluso si el equipo está apagado.

El Sistema Operativo deberá ser compatible 100% con al menos alguna de las siguientes versiones de Sistema Operativo:
- Oracle Solaris 11.1
- Oracle Solaris 10 1/13 más actualización de parches

Soporte para Sistemas Operativos Guest:
- Oracle Solaris 11.1
- Oracle Solaris 10 1/13 *
- Oracle Solaris 10 8/11 *
- Oracle Solaris 10 9/10 *
- Si la base es IBM:
  - AIX Versión 7.1 *
  - AIX Versión 6.1 *
- Si la base es HP
  - HP-UX 11i v3 *

* Más actualización de parches

ANEXOS

DIVISIÓN DE CONTRATOS

2.1.1.1.2. Servidor X86 Modalidades M1, M2, M3, M5 y M6

El Procesador deberá ser de al menos alguna de las siguientes familias:

- Intel® Xeon® Processor E7 v3 o superior
  - Cache de 20MB a 45MB
  - Velocidad de 1.90GHz a 3.20GHz
- Intel® Xeon® Processor 7000 Sequence
  - Cache de 4MB a 24MB
  - Velocidad de 1.90GHz a 3.20GHz

Y deberá ser escalable con al menos incrementos de:
- Módulos de 1 Procesador con 32 threads

La memora RAM BASE deberá ser cuando menos de:
- 128 GB de memoria RAM

Y deberá tener incrementos de cuando menos:
- 128 GB de memoria RAM

El chasis deberá estar optimizado para rack (De 1 unidad de rack) y que cuente con los rieles y accesorios necesarios para conectarse a un rack de 42U.

El adaptador de bus del host (HBA) deberá tener al menos 4 tarjetas para:
- 2 para soporte a la SAN velocidad mínima 10 Gbps (FC, ISCSI o FCoE)
- 2 para respaldo velocidad mínima 10 Gbps Ethernet

La Interface de video deberá estar Integrada a la tarjeta madre.

La tarjeta de red deberá incluir por lo menos 4 puertos de red RJ45, velocidad 10 Gigabit Ethernet.
La Unidad de DVD-R / CD-RW deberá estar Incluido.

El Disco Duro deberá tener al menos 2 discos duros SAS de 500 GB de capacidad, velocidad mínima de 15000 rpm.

El servidor y los discos duros deben soportar la característica Hot Plug.

La fuente de poder deberá contar al menos con 2 fuentes internas de poder hot plug redundantes.

El sistema deberá incluir conexión eléctrica para conectores tipo NEMA 5-15R, a 127 volts y 60 Hz.
En caso de traer otro tipo de conector, el Proveedor deberá implementar sin costo para el Instituto el tipo de conector eléctrico que requiera la solución que oferta.

Deberá incluir al menos un puerto de conexión al teclado, al mouse y otro al monitor.

Deberá incluir al menos 2 puertos USB libres sin considerar las conexiones de teclado y mouse.

Contar con password de arranque y password de setup de BIOS.

Deberá contar al menos con 2 ventiladores internos.

Deberá contar con tarjeta de administración remota que permita la administración del mismo en una interfaz de modo texto, incluso si el equipo está apagado.

El Sistema Operativo deberá ser compatible, entre otras, con las siguientes versiones de Sistema Operativo:

- Oracle Linux 5X, 6X o 7X
- Windows Server 2008 / 2012 / 2014
- Diferentes Distribuciones Linux

2.1.1.1.3. Módulo de Seguridad en Hardware (HSM)

Especificaciones del Módulo de Alta seguridad Criptográfica (HSM)
Niveles de Seguridad Mínimos

- Certificación FIPS 140-2 Nivel 3
- Common Criteria EAL 4+

Especificaciones Funcionales Mínimas

- Almacenamiento y procesamiento de llaves criptográficas
- Cifrado de llaves simétricas (DES, 3DES de dos y tres claves, SAFER, AES, ARIA, CAST) en modos:
  - ECB
  - CBC
  - CFB-64
  - OFC-64
- Hash (MD5, SHA-1, SHA-2, (224, 256, 384, 512), RIPEMD) en 128 y 160 bit
- Llaves RSA de hasta 4096 bits, Diffie-Hellman.
- Time Control
- Control de acceso multinivel autenticado
- Duty Segregation (Administrador y operador)
- Almacenamiento no limitado de llaves
- Generación de claves mediante random number generator de acuerdo a FIPS 186-2

Especificaciones Técnicas Mínimas

- Dos coprocesadores RSA
- Coprocesador simétrico
- Protección anti-tampering de la tarjeta HSM (sensores al menos para temperatura, acceso físico, tensión)
- Generación de números aleatorios por hardware

- Puertos Gigabit Ethernet
- Interfaz PCI 2.1

Medios de almacenamiento de acceso directo

2.1.1.1.4. Almacenamiento de Datos Individual

Se requiere el servicio de Almacenamiento de Datos con espacio inicial de 500 GB utilizables considerando el uso de RAID 5 con las siguientes características:

- El almacenamiento debe ser de alta disponibilidad
- Tener la capacidad de interconexión InfiniBand de 56 Gbps.
- Tener la capacidad como mínimo manejar los siguientes protocolos:
  - FC: 4 de 8 Gbs (FC, SRDF)
  - FC: 4 de 16 Gbs (FC, SRDF)
  - GbE: 2/2 óptico/cobre (SRDF)
  - 10 GbE: 2 de 10 GbE (SRDF)
- Soportar al menos los siguientes tipos de unidades de disco:
  - SAS de 3.5in de 300GB, 600GB, 1.2TB a 10krpm.
  - SAS de 3.5in de 300GB a 15krpm.
  - SAS flash de 3.5in de 200GB, 400GB, 800GB, 1.6TB.
  - SAS de 2.5in de 300GB, 600GB, 1.2TB a 10krpm.
  - SAS de 2.5in de 300GB a 15krpm.
- Ser compatible con la plataforma Mainframe.
- Ser compatible con compresión SRDF a través de hardware:
  - Gbe/10 GbE
  - FC de 8 Gb/s
  - FC de 16 Gb/s

El servicio deberá tener la capacidad de poder configurar almacenamiento por red (NAS) con las siguientes características:

- Permitir el consumo de recursos de manera uniforme.
- Tener la capacidad de ser compatible con al menos:
  - GbE: 4 de 1 GbE de cobre.
  - 10 GbE: 2 de 10 GbE de cobre.
  - 10 GbE: 2 de 10 GbE óptico.
  - FC: 4 de 8 Gbs (respaldo NDMP).

El servicio deberá incluir todo el licenciamiento de software requerido para cumplir con los requerimientos siguientes:

- Incluir herramientas de migración y habilitadoras.
- Aprovisionamiento de SLOs tanto para bloque como para archivo.

- Tener la capacidad de realizar optimizaciones automáticas para obtener el mejor rendimiento del sistema.
- Permitir la creación de snapshots y clones con impacto nulo.

Permitir la protección de datos y aplicaciones de modo síncrono, asíncrono y clúster, así como replicación de archivos.

- Permitir la operación en cascada desde un sitio primario a múltiples sitios remotos.
- Permitir que las aplicaciones puedan iniciar respaldos directos entre el arreglo de discos y la solución de respaldos de manera simple y rápida.
- Proporcionar acceso simultáneo de LUN/grupos de almacenamiento para acceso de datos sin interrupción y disponibilidad.

El equipo debe permitir la continuidad de la operación en caso de cualquier contingencia.

En caso de falla de algún componente del equipo utilizado por el proveedor, el contenido almacenado debe poder regenerarse utilizando los niveles de protección solicitados.

El servicio debe contar con borrado seguro con certificado cada vez que se reemplace un disco por mantenimiento, por actualización tecnológica a nuevos equipos durante la vida del contrato y al término del contrato.

Incremento

El Instituto podrá solicitar el Incremento de la capacidad del equipo ofrecido para el almacenamiento de Datos en al menos 100GB para cualquiera de las siguientes opciones:

- Discos de estado sólido
- Discos FC
- Discos SATA

Lo anterior en arreglo RAID 5

2.1.1.1.5. Respaldo de Datos Individual

Se requiere el servicio para el sistema de respaldos de Datos con las siguientes caracteristicas:

- Contar con protección de tipo mínimo RAID 6
- Garantizar el mejor aprovechamiento de las redes de conectividad LAN y SAN, sistema de respaldo de datos debe contar con conectividad FC y Ethernet, basada en discos SAS, con funciones de deduplicación interna y replicación vía enlace IP.
- Garantizar que la pérdida de un disco en la unidad de almacenamiento no genere la pérdida de información, ésta deberá estar configurada con una protección de al menos RAID 6, con al menos un disco de hotspare.
- Garantizar la disponibilidad y su mantenimiento no disruptivo dando continuidad al servicio de respaldo y restauración.

- Utilizar algoritmos de deduplicación para almacenar la información.
- Cumplir con las siguientes características que permitan mejorar el uso del espacio:
  - La deduplicación de los datos respaldados debe ser "en línea", esto es, no debe realizarse en un proceso posterior.
  - El proceso de deduplicación no debe requerir de un espacio en disco temporal.
  - El proceso de deduplicación deberá poder distribuirse en el origen y en el destino a través de los protocolos Ethernet y Fiber Channel
- Contar con la posibilidad de recuperar la información en un sitio alterno en caso de que el sitio principal presente algún problema que impida la operación.
- Permitir la replicación de datos entre dos o más equipos a través de la WAN y la replicación debe satisfacer los siguientes requerimientos:
  - Replicar datos deduplicados: es decir la replicación debe ocurrir después de los procesos de deduplicación con el objeto de minimizar la cantidad de datos a enviar a través de la WAN y por ende demandar un menor ancho de banda para el proceso de replicación.
  - La replicación debe ser bidireccional, es decir de un equipo local a otro equipo remoto y viceversa.
- Cumplir los tiempos de respaldo y de restauración de la información en la unidad de almacenamiento.
- Soportar su configuración como VTL (Virtual Tape Library) y conectarse directamente a la SAN

El equipo debe permitir la recuperación mediante snaps y clones

El equipo deberá incluir todo el licenciamiento de software necesario para cumplir con los requerimientos

En caso de falla de algún componente del equipo utilizado el contenido almacenado debe poder regenerarse utilizando los niveles de protección solicitados.
El equipo debe contar con borrado seguro con certificado cada vez que se reemplace un disco por mantenimiento, por actualización tecnológica a nuevos equipos, durante la vida del contrato y al término del contrato.

2.1.1.1.6. Unidad de almacenamiento para archivado de contenido

Se requiere el servicio de almacenamiento para archivado de contenido, por lo que el equipo deberá tener las siguientes caracteristicas:

- El equipo deberá contar con un espacio base usable de 60TB como mínimo para garantizar su operación durante la vida del contrato
- Debe ser de tipo CAS
- Debe poder incrementarse conforme el Instituto así lo requiera

ANEXOS

DIVISIÓN DE CONTRATOS

- La protección a la información que se encuentra en el almacenamiento de tipo CAS debe estar protegida con el tipo RAIN (Redundant Array of Independent Nodes por sus siglas en inglés)
- Para el adecuado cumplimiento de las diferentes regulaciones existentes el almacenamiento de la información deberá realizarse precisando distintos periodos de retención definidos por la dependencia o indefinidos en caso de que así se especifique, de tal manera que se garantice la permanencia de la información.
- Se requiere guardar y recuperar la información con base en el contenido de los objetos almacenados, proporcionando una única dirección de contenido a cada objeto almacenado derivada del mismo contenido.
- Permitir que el acceso a la información almacenada sea en línea.

El almacenamiento tipo CAS deberá

- Almacenar la información utilizando al menos los siguientes esquemas de protección:
  - Protección del contenido en Espejo
  - Protección del contenido por paridad.
- Contar con mecanismos que no permitan que la información sea modificada.
- Poder manejar los periodos de retención que sean definidos para el contenido que se está almacenando.
- No permitir modificar el periodo de retención del contenido, una vez que el contenido sea grabado.
- Tener la capacidad de poder eliminar completamente la información que sea borrada, mediante la utilización de mecanismos que garanticen que la información que ha sido borrada no se pueda recuperar (borrado seguro).
- Tener la capacidad de replicar la información contenida a otro almacenamiento del mismo tipo por IP, de manera remota y asíncrona, garantizando el acceso al contenido que sea replicado para protección frente a un desastre.
- Poder aceptar contenido de diferentes aplicaciones de manejo de contenidos, aplicaciones de digitalización de imágenes, correo electrónico, call centers, video, entre otros.
- Soportar el adicionamiento de aplicaciones sin necesidad de reconfiguración del sistema de almacenamiento.
- Estar diseñado para el manejo de información que no cambia en el tiempo.
- Permitir que el mismo contenido sea referenciado por múltiples usuarios concurrentes y manteniendo la disposición del primer byte en menos de un segundo después de recibida la solicitud.
- Permitir la recuperación del contenido de la información de objetos en condiciones de fallas del equipo.
- Detectar cuando dos copias idénticas del mismo objeto están siendo almacenadas y evitar la duplicidad de información.
- Tener capacidad de migrar datos de manera automática a tecnología más moderna mediante un proceso desatendido que no impacte a los aplicativos.
- Tener capacidad de integrarse a sistemas de respaldo mediante el protocolo NDMP.

- La ubicación de los objetos almacenados por la aplicación debe llevarse a acabo mediante el uso de la dirección por contenido asignada durante el proceso de escritura.
- Contar con un mecanismo automatizado para las gestiones correspondientes al balanceo de cargas, auto-corrección, auto diagnóstico, determinación de autenticidad y/o perdida de información.

El equipo deberá incluir todo el licenciamiento de software requerido para cumplir con los requerimientos.

En caso de falla de algún componente del equipo utilizado por el proveedor, el contenido almacenado debe poder regenerarse utilizando los niveles de protección solicitados.

El equipo deberá contar con borrado seguro con certificado cada vez que se reemplace un disco por mantenimiento, por actualización tecnológica a nuevos equipos, durante la vida del contrato y al término del contrato.

Incremento

El Instituto podrá solicitar el crecimiento de la capacidad del equipo ofrecido para el almacenamiento para archivado de contenido en bloques de 24 Terabytes

2.1.1.1.7. Unidad de almacenamiento de media categoría para aplicaciones de bajo desempeño

Se requiere el servicio de almacenamiento de media categoría para almacenar todo lo correspondiente a equipos virtualizados, por lo que el equipo deberá tener las siguientes características:

- El equipo deberá contar con un espacio base de 90TB con protección de RAID 5 considerando las políticas de respaldo y retención del Instituto
- Contar con la capacidad de mover los datos entre las diferentes tecnologías de disco de forma automatizada.
- Proveer volúmenes a distintos tipos y marcas de sistemas operativos, por ejemplo: HP-UX, IBM AIX, Solaris, Linux, Windows, Citrix (Xen), MacOS, VMware, VMware vSphere, VMware ESX, VMware vCenter Server
- El equipo deberá tener la capacidad de integración de réplica y recuperación de tipo DVR de punto en el tiempo, con un sistema CDP (local), CRR (remota)
- El equipo deberá tener la capacidad de integración de protección de réplica en donde se alcance el valor de RPO =0
- El equipo deberá tener la capacidad de integración de replicación sobre IP a cualquier distancia y contar con protección durante falla de link WAN.
- El equipo deberá tener la capacidad de integración a replica donde se reduzcan costos de comunicación (anchos de banda)

El equipo deberá incluir todo el licenciamiento de software requerido para cumplir con los requerimientos siguientes:

- Capacidad de replicación de volumen local a nivel de bloque y a nivel de archivo. Modo asincrono, unidireccional y bidireccional.
- Capacidad de realizar movimiento de datos dentro del mismo sistema de acuerdo al requerimiento de desempeño y/o por medio de políticas en diferentes niveles (tiers) de disco, dicho movimiento de información debe de ser de cuando menos 256MB
- Capacidad de migración de volúmenes de thick a thin y viceversa.
- Capacidad de soportar volúmenes NAS mixtos (CIFS y NFS) para ambientes Windows y Linux, entre otros, así como la funcionalidad a futuro de entregar volúmenes NAS a través de puertos FC o SAN.
- Capacidad de crear clones de volúmenes y snapshots.
  - hasta 8,000 snapshots para todo el sistema
  - hasta 256 snapshots por LUN
- Software o tecnologia integrada para la optimización del almacenamiento mediante la compresión y deduplicación a nivel de bloque
- Software o tecnologia integrada para la optimización del almacenamiento mediante la deduplicación y compresión a nivel de archivo.
- Software de encriptación de datos a nivel de bloques, como funcionalidad a futuro.
- Software para el manejo y retención de archivos, como funcionalidad a futuro
-

En caso de falla de algún componente del equipo utilizado por el proveedor, el contenido almacenado debe poder regenerarse utilizando los niveles de protección solicitados.

El equipo deberá contar con borrado seguro con certificado cada vez que se reemplace un disco por mantenimiento, por actualización tecnológica a nuevos equipos, durante la vida del contrato y al término del contrato

Incremento

El Instituto podrá solicitar el crecimiento de la capacidad del equipo ofrecido para el almacenamiento de media categoría para almacenar todo lo correspondiente a equipos virtualizados en al menos, cualquiera de las siguientes opciones:

- Discos de estado sólido 1TB usable como mínimo
- Discos FC 1TB usable como mínimo
- Discos SATA 1TB usable como mínimo

Lo anterior en arreglo RAID 5.

2.1.1.1.8. Unidad de respaldo de plataforma abierta

Se requiere el servicio de respaldo de aplicaciones desarrolladas en plataforma abierta, por lo que el equipo deberá tener las siguientes características:

- Contar con una capacidad base usable de almacenamiento de al menos 90TB con protección de tipo mínimo RAID 5
- Garantizar el mejor aprovechamiento de las redes de conectividad LAN y SAN, el almacenamiento debe contar con conectividad FC y Ethernet, basada en discos SAS, con funciones de deduplicación interna y replicación via enlace IP.
- Garantizar que la pérdida de un disco en la unidad de almacenamiento no genere la pérdida de información, ésta deberá estar configurada con una protección de al menos RAID 6, con al menos un disco de hotspare.
- Garantizar la disponibilidad y su mantenimiento no disruptivo dando continuidad al servicio de respaldo y restauración.
- Utilizar algoritmos de deduplicación para almacenar la información.
- Cumplir con las siguientes características que permitan mejorar el uso del espacio:
  - La deduplicación de los datos respaldos debe ser "en línea", esto es, no debe realizarse en un proceso posterior.
  - El proceso de deduplicación no debe requerir de un espacio en disco temporal.
  - El proceso de deduplicación deberá poder distribuirse en el origen y en el destino a través de los protocolos Ethernet y Fiber Channel
- Contar con la posibilidad de recuperar la información en un sitio alterno en caso de que el sitio principal presente algún problema que impida la operación.
- Permitir la replicación de datos entre dos o más equipos a través de la WAN y la replicación debe satisfacer los siguientes requerimientos:
  - Replicar datos deduplicados: es decir la replicación debe ocurrir después de los procesos de deduplicación con el objeto de minimizar la cantidad de datos a enviar a través de la WAN y por ende demandar un menor ancho de banda para el proceso de replicación.
  - La replicación debe ser bidireccional, es decir de un equipo local a otro equipo remoto y viceversa.
- Cumplir los tiempos de respaldo y de restauración de la información en la unidad de almacenamiento.
- Soportar su configuración como VTL (Virtual Tape Library) y conectarse directamente a la SAN contando con la capacidad de emulación de al menos 64 diferentes Librerías Virtuales de Cinta, 500 diferentes Drives de Cinta y 6000 Cintas virtuales.

El equipo debe permitir la recuperación mediante snaps y clones
El equipo deberá incluir todo el licenciamiento de software requerido para cumplir con los requerimientos.
En caso de falla de algún componente del equipo utilizado por el proveedor, el contenido almacenado debe poder regenerarse utilizando los niveles de protección solicitados.
El equipo debe contar con borrado seguro con certificado cada vez que se reemplace un disco por mantenimiento, por actualización tecnológica a nuevos equipos, durante la vida del contrato y al término del contrato

Incremento

El Instituto podrá solicitar el crecimiento de la capacidad del equipo ofrecido para el respaldo de aplicaciones desarrolladas en plataforma abierta en bloques de 30TB usables en arreglo RAID 5

2.1.1.1.9. Unidad de almacenamiento de datos de alto rendimiento y red SAN

Se requiere el servicio de almacenamiento de Datos de alto rendimiento y red SAN, por lo que el equipo deberá contar con las siguientes características:

- Contar con al menos 2 switches de tipo director de por lo menos 384 puertos cada uno y que cada puerto sea de al menos 16 GBps.
- Contar con una capacidad base de almacenamiento de al menos 90TB utilizables con protección de tipo mínimo RAID 5
- Ser un almacenamiento de alta disponibilidad.
- Contar con tecnología de interconexión InfiniBand de 56 Gb/s.
- Los módulos de SAN deben de tener la capacidad como mínimo manejar los siguientes protocolos:
  - FC: 4 de 8 Gbs (FC, SRDF)
  - FC: 4 de 16 Gbs (FC, SRDF)
  - GbE: 2/2 óptico/cobre (SRDF)
  - 10 GbE: 2 de 10 GbE (SRDF)
- Soportar al menos los siguientes tipos de unidades de disco:
  - SAS de 3.5in de 300GB, 600GB, 1.2TB a 10krpm.
  - SAS de 3.5in de 300GB a 15krpm.
  - SAS de 3.5in de 4TB a 7.2krpm.
  - SAS flash de 3.5in de 200GB, 400GB, 800GB, 1.6TB.
  - SAS de 2.5in de 300GB, 600GB, 1.2TB a 10krpm.
  - SAS de 2.5in de 300GB a 15krpm.
  - SAS flash de 2.5in de 200GB, 400GB, 800GB, 1.6TB.
- Permitir la configuración de por lo menos los siguientes RAID:
  - RAID 1: Todas las unidades.
  - RAID 5: (3 + 1) o (7 +1) para todas las unidades.
  - RAID 6: (6 + 2) o (14 + 2) para todas las unidades.
- Ser compatible con la plataforma Mainframe.
- Ser compatible con compresión SRDF a través de hardware:
  - Gbe/10 GbE
  - FC de 8 Gb/s
  - FC de 16 Gb/s

El equipo deberá tener la capacidad de poder configurar almacenamiento por red (NAS) con las siguientes características:

- Permitir el consumo de recursos de manera uniforme.

- Tener la capacidad de ser compatible con al menos:
  - GbE: 4 de 1 GbE de cobre.
  - 10 GbE: 2 de 10 GbE de cobre.
  - 10 GbE: 2 de 10 GbE óptico.
  - FC: 4 de 8 Gbs (respaldo NDMP).
  - (máx. 1/Data Mover de software).

El equipo deberá incluir todo el licenciamiento de software requerido para cumplir con los requerimientos siguientes:

- Incluir herramientas de migración y habilitadoras.
- Aprovisionamiento de SLOs tanto para bloque como para archivo.
- Tener la capacidad de realizar optimizaciones automáticas para obtener el mejor rendimiento del sistema.
- Permitir la creación de snapshots y clones con impacto nulo.
- Permitir la protección de datos y aplicaciones de modo síncrono, asíncrono y clúster, así como replicación de archivos.
- Permitir la operación en cascada desde un sitio primario a múltiples sitios remotos.
- Permitir que las aplicaciones puedan iniciar respaldos directos entre el arreglo de discos y la solución de respaldos de manera simple y rápida.
- Permitir la ampliación del servicio de datos automatizando el almacenamiento de arreglos externos.
- Proporcionar acceso simultáneo de LUN/grupos de almacenamiento para acceso de datos sin interrupción y disponibilidad.

El equipo debe permitir la continuidad de la operación en caso de cualquier contingencia.
En caso de falla de algún componente del equipo utilizado por el proveedor, el contenido almacenado debe poder regenerarse utilizando los niveles de protección solicitados.

El equipo debe contar con borrado seguro con certificado cada vez que se reemplace un disco por mantenimiento, por actualización tecnológica a nuevos equipos durante la vida del contrato y al término del contrato

Incremento

El Instituto podrá solicitar el crecimiento de la capacidad del equipo ofrecido para el almacenamiento de Datos de alto rendimiento y red SAN en al menos, cualquiera de las siguientes opciones:

- Discos de estado sólido 1TB usable como mínimo
- Discos FC 1TB usable como mínimo
- Discos SATA 1TB usable como mínimo

Lo anterior en arreglo RAID 5

2.1.1.1.10. Unidad de almacenamiento de alto rendimiento para bases de datos Oracle y Microsoft SQL

Se requiere el servicio de una solución de una unidad de almacenamiento de alto rendimiento en discos SSD (estado sólido) con deduplicación y compresión en línea para lograr el máximo rendimiento posible. La misma debe cumplir con los requisitos técnicos mínimos detallados a continuación:

- La solución debe permitir su escalabilidad en nodos permitiendo formar clusters con múltiples nodos interconectados por una red Infiniband de 40Gbps. La solución inicialmente deberá constar de un único nodo, pero podrá crecer a 2, 4,6 y hasta 8 nodos en un solo cluster.
- Cada nodo de almacenamiento debe contar con dos controladoras redundantes entre sí, baterías de respaldo, y un DAE para 25 discos duros de estado sólido.
- Cada controladora debe poseer su propio procesamiento, memoria y tarjetas de conectividad para asegurar un crecimiento lineal del desempeño al agregar nuevos nodos al cluster
- Cada controladora debe incluir al menos 2 puertos de FC 8Gbps y 2 puertos de red iSCSI Ethernet (10Gbps). De esta forma el nodo contaría con un total de 4 puertos de cada tipo de puerto descrito anteriormente.
- Cada controladora debe incluir al menos un puerto de administración de 1Gb Ethernet.
- Cada nodo debe ser capaz de entregar 150,000 IOPS contemplando un patrón de IO de 70% lecturas y 30% escrituras en bloques de 8K. El oferente debe entregar documentación técnica del fabricante que respalde este punto.
- Cada nodo debe ser capaz de entregar una latencia promedio de 0.5ms contemplando un patrón de IO de 70% lecturas y 30% escrituras en bloques de 8K. El oferente debe entregar documentación técnica del fabricante que respalde este punto.
- Cada controladora y el DAE del nodo debe contar con fuentes de poder redundantes
- El nodo debe contar con almacenamiento de 10TB crudos (7.6TB utilizables) con la capacidad para entregar 35TB lógicos a través de la deduplicación con una tasa 5 a 1
- La solución debe soportar la creación de volúmenes Thin Provisioning
- El nodo ofertado no debe ser superior a las 6U de altura como máximo
- La solución debe estar basada en una arquitectura completamente diseñada y dedicada al uso de discos duros SSD, que permita sacarle el máximo desempeño, durabilidad y capacidad a estos discos, por lo que no se aceptarán arreglos híbridos de propósito general que hayan sido configurados con discos duros de SSD
- El nodo ofertado debe venir con al menos 25 discos de 400GB SSD eMLC
- La solución debe contar con mecanismos para la prolongación de la vida de los SSD, que minimicen la cantidad de escrituras necesarias en los discos desacelerando la degeneración de los mismos
- La solución debe ser altamente disponible sin puntos únicos de falla
- La solución debe tener habilitada y siempre encendida la función de deduplicación en línea, que identifique y escriba en los discos solo bloques únicos de datos, optimizando la

capacidad física instalada y aumentando la durabilidad de los discos. No se aceptarán soluciones con deduplicación post-proceso

- Debe incluir su propio Sistema Operativo sin encarecer la oferta
- Debe soportar los protocolos: iSCSI y Fibre Channel
- La solución debe ser capaz de efectuar snapshots y clones de los volúmenes
- La solución debe soportar un mecanismo de proteccion de discos N+2, sin necesidad de hot spares, permitiendo al equipo reconstruir la data del disco fallido de forma diluida entre los demás discos
- Debe ser Compatible con los Sistemas Operativos Windows Server 2008/2012 y RHEL 5.x, 6.x
- Debe ser compatible con los hypervisores VMware ESX Server, Citrix XenServer, Microsoft Hyper-V
- Debe soportar integración avanzada con el VMWare VAAI (vStorage APIs for Array Integration), soportando funciones como "block zeroing", "XCOPY", "ATS" y "unmap", permitiendo desligar a los hosts de operaciones relacionadas con el almacenamiento, y acelerando dramáticamente operaciones como el clonado de máquinas virtuales
- Debe ser compatible con los gestores de Base de Datos Microsoft SQL Server, Oracle
- La solución debe poder reportar su estado y enviar alertas en caso de fallo las cuales deben ser enviadas a una cuenta de correo mediante los protocolos SMTP y SNMP
- La solución debe soportar las siguientes certificaciones: RoHS, CE, UL, FCC/EMC

Incremento

El Instituto podrá solicitar el crecimiento de la capacidad de la unidad de almacenamiento de alto rendimiento en discos SSD (estado sólido) con deduplicación y compresión en linea en al menos, discos de estado sólido con 2 nodos de 25 discos de 400 GB como mínimo

2.1.1.1.11. Sistema de Almacenamiento de Datos

El servicio incluye la infraestructura para cumplir con el requerimiento del Instituto para contar con 12TB utilizables. Los gastos de instalación y configuración están considerados en el cálculo del precio mensual.

- El Proveedor deberá considerar en su propuesta que el sistema de almacenamiento de datos puede ser dedicado o compartido. Para el caso de que su propuesta sea equipo dedicado 100% al Instituto los aspectos de seguridad a considerar son los aspectos físicos en cuanto a accesos, cerraduras, controles varios, etc. Para el caso de que su propuesta sea equipo compartido, el Proveedor deberá asegurar, además de los aspectos físicos, que ninguno de los elementos de hardware asignados pueda ser accedido por personas ajenas al Instituto y que no tengan que ver con la administración del mismo, por ende se

ANEXOS
DIVISIÓN DE CONTRATOS

entiende que tampoco habrá acceso a la información del Instituto por parte de dichas personas.

- El equipo deberá incluir al menos 12 Terabytes utilizables en arreglo RAID 5 y tener un crecimiento de hasta al menos 23 Terabytes utilizables en RAID 5, con discos de fibra a 15,000 RPM.
- El equipo deberá ser capaz de manejar al menos niveles de RAID 0, 1, y 5, deberá soportar en sí mismo la combinación de cualquiera de estos arreglos.
- El equipo deberá soportar al menos los siguientes tipos de discos 146 GB a 15,000 rpm, 300 GB a 15,000 rpm, 450 GB a 10,000rpm; o tecnologías equivalentes disponibles en el mercado.
- Para el soporte a los 12 Terabytes se deberán proveer discos de al menos 300 GB de capacidad, a 15000 RPM, tipo Fibre Chanel.
- Todos los discos deberán tener doble puerto de acceso para accesos redundantes para el caso de que un puerto falle.
- El equipo deberá contar al menos con 4 GB de memoria caché con protección.
- El equipo deberá contar con un respaldo de baterías para la memoria caché con suficiente capacidad que garantice que la información almacenada en memoria caché sea grabada en el disco duro.
- El equipo deberá ser capaz de operar en entornos de SAN.
- El equipo deberá permitir tecnología Fibre Chanel en el sistema, o tecnología equivalente disponible en el mercado.
- Todos los componentes del sistema: Fuentes de alimentación, controladoras, discos duros; deberán tener la capacidad de ser reemplazados de manera no disruptiva.
- El equipo deberá contar con capacidad de aislamiento de fallas y disco spare.
- El equipo deberá contar con las tarjetas y circuitería necesaria para la conexión al 100 por ciento a la SAN en un esquema redundante (Equipo de Interconexión SAN considerados en el punto 5.6 del equipamiento remoto).
- El equipo deberá contar al menos con dos fuentes de poder redundantes y ventiladores de enfriamiento redundantes por cada enclosure de discos que maneje, o bien, un sistema de enfriamiento para toda la plataforma.
- El equipo deberá venir con un rack de montaje en piso.
- El equipo deberá contar con un módulo de Optimización Automático del Sistema de Almacenamiento: Se deberán proporcionar las licencias adicionales para la optimización de volúmenes, las cuales deberán contar con al menos las siguientes características :
    - Deberá permitir el balanceo automático entre los paths de acceso hacia los datos.
    - Se deberá incluir el software y el licenciamiento necesario para la correcta operación del equipo y el cumplimiento de los Niveles de Servicio
- El equipo deberá contar con un software que se cargue en un servidor Windows o Unix para establecer la consola o estación que permita administrar, configurar y vigilar el comportamiento y el rendimiento de la unidad de almacenamiento en su conjunto, o bien, si el equipo lo permite, este software podrá venir instalado en el mismo equipo y deberá poder ser administrado desde una interfaz Web.

- El equipo deberá permitir el control y el manejo de alertas en forma proactiva, el software debe mostrar el comportamiento de todos los componentes físicos de la unidad (discos, canales, ventiladores, etc.).
- El equipo deberá contar con un sistema de auto monitoreo interno 7x24x365. El monitoreo deberá ser proactivo y predictivo y deberá proveer la facilidad de reportar automáticamente las fallas a un centro de monitoreo local y remoto. El Proveedor debe contar con este centro de monitoreo ya sea en sus instalaciones o a través de un servicio con el fabricante del Sistema de Almacenamiento, de modo que las alertas que genere el equipo sean atendidas y en caso de ser necesario dar aviso al personal del Instituto y al personal que designe el Proveedor.
- El equipo deberá contar con una línea de comandos que permita obtener información de la unidad de almacenamiento.
- El equipo deberá contar con una conexión Ethernet LAN para poder ser administrado.
- El equipo deberá tener la capacidad de ser administrado a través de SNMP, Telnet o a través de WEB. La conexión por telnet se refiere a tareas administrativas o de operación sobre el equipo, que generalmente hacen técnicos especializados del fabricante y/o centros de servicio.
- El equipo deberá contar con software que deberá venir ya configurado para las siguientes actividades:
    - Permitir una administración centralizada.
    - Permitir el análisis y configuración de espacios para optimización del performance de las aplicaciones.
    - Facilitar el análisis de performance de discos, por controladora, puertos del sistema de almacenamiento y HBAs.
    - Permitir la asignación dinámica de volúmenes.
    - Permitir la generación de reportes del performance del equipo.
    - Permitir el monitoreo continuo del equipo.
- El Proveedor deberá ofertar las licencias de todo el software preinstalado en el equipo así como el solicitado.
- El Proveedor deberá incluir un servidor del tipo rack para administrar tanto la solución de almacenamiento como la solución de respaldo, las características de este equipo, serán al menos las solicitadas para el servidor de mediano rendimiento de tal forma que el servidor que se proponga para ese requisito será el que se deberá asignar a este punto, o bien otro, pero que cumpla con las características mínimas solicitadas.
- La configuración de almacenamiento deberá proporcionar o mostrar a cada servidor conectado a la SAN sólo los LUNs que tenga que ver cada servidor, esta definición se hará entre el Instituto y el Proveedor.

Incremento del Sistema de Almacenamiento de Datos

Se requiere tener un precio de incrementos en unidades 100GB para que el Instituto pueda solicitar asignación de mayor espacio en disco de acuerdo a sus necesidades de espacio durante la vigencia del contrato.

Medios de almacenamiento extraíbles

2.1.1.1.12. Unidad individual de respaldos (Portatil)

Se requiere el servicio de un equipo de unidad de respaldos portátil, el cual deberá tener las siguientes características:

- El procesador Intel Celeron Processor (2.58GHz, Dual-Core) o superior
- Memoria deberá ser AGB DDR3L SODIMM o superior
- Tamaño y tipo del disco duro: 3.5" SSD con una capacidad de almacenamiento de al menos 10 TB
- una fuente de poder de 100~240 V AC
- Ventiladores de cuando menos 2 x 120mm
- Soportar los siguientes buscadores:
  - Internet Explorer 9 Onwards,
  - Firefox, Chrome,
  - Safari
- Soportar los siguientes sistemas de archivos:
  - Internal Disk: EXT4 (sistema de archivos transaccional)
  - External Disk: FAT32 o NTFS o EXT3 o EXT4 o HFS+
- Permitir la administración para
  - Support Multiple Volumes with Spare Disks
  - Volume Type: RAID 1
- Contar con 4x Gigabit Ethernet Ports
- Manejar los siguientes protocolos:
  - CIFS/SMB,
  - AFP,
  - NFS,
  - FTP,
  - WebDAV,
  - Rsync, SSH,
  - SFTP,
  - iSCSI,
  - HTTP,
  - HTTPS,
  - SMB 2.0,
  - TFTP,
  - Proxy
- Manejar las siguientes modalidades:
  - System Automatically Enters Sleep Mode (Schedule S3)
  - Auto-Standby for Both Internal and External Disks

  - Auto Fan Control
  - LED Night Mode
  - Power Schedule: On, Off, Restart, and Sleep

2.1.2. Sistema Operativo

Servidores de medio desempeño

2.1.2.1.1. Sistema Operativo Red Hat Enterprise Linux

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma RED HAT ENTREPRISE LINUX SERVER o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

Para este servicio se considerarán los Bloques de Construcción Fundamentales sobre el producto RED HAT ENTREPRISE LINUX SERVER, de acuerdo a lo que se especifica en el Apéndice correspondiente.

- Software de RED HAT ENTREPRISE LINUX SERVER o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 6 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

2.1.2.1.2. Sistema Operativo Debian

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma LINUX DEBIAN o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

Para este servicio se considerarán los Bloques de Construcción Fundamentales sobre el producto LINUX DEBIAN, de acuerdo a lo que se especifica en el Apéndice correspondiente.

- Software de LINUX DEBIAN o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 6 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

2.1.2.1.3. Sistema Operativo SLES

El instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma SUSE LINUX ENTERPRISE SERVER o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de SUSE LINUX ENTERPRISE SERVER o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 10 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

2.1.2.1.4. Sistema Operativo CentOS

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma CentOS o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de CentOS Subscription o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 6 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

2.1.2.1.5. Sistema Operativo Ubuntu

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma UBUNTU o equivalente según sus necesidades.El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de UBUNTU Subscription o equivalente (soporte empresarial que incluye Indemnización legal)
- Version del producto 14 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

2.1.2.1.6. Sistema Operativo Oracle Linux Server

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma ORACLE SERVER LINUX o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación en esta plataforma.

Requerimientos Mínimos:

- Subscripción de soporte de ORACLE SERVER LINUX (6 o superior) o equivalente (soporte empresarial 7/24 en línea y presencial con el mismo nivel de servicio que ofrece el Centro de Datos)
- Aplicación de actualizaciones y parches (releases/bugfixes)
- Acceso a bases de conocimiento del fabricante
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

2.1.2.1.7. Sistema Operativo Windows Server 2008

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Windows Server 2008 o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Windows Server 2008 o equivalente (soporte empresarial)
- Version del producto 2008 R1 (estándar y Enterprise) y posteriores

- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

2.1.2.1.8. Sistema Operativo Windows 2012

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Windows 2012 o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Windows 2012 o equivalente (soporte empresarial)
- Version del producto 2012 R1 (estándar y datacenter) y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

2.1.3. Plataformas de virtualización

Servidores

2.1.3.1.1. Servidor virtual RISC Modadlidad M1, M2 y M6

El Procesador deberá tener al menos alguna de las siguientes arquitecturas BASE:

- Oracle SPARC T5-8 Server
  - SPARC T5 16-cores a 3.6 GHz
  - 128 threads por procesador
  - Cache 8 MB compartidos, Level 3 Cache; 128 KB Level 2
- IBM Power Systems Enterprise Servers
  - 24 to 48 cores (12-core) a 3.72 GHz
- HP Integrity Servers
  - 16 processors/240 cores a 2.8 GHz

Y deberá ser escalable con al menos incrementos de:

- Módulos de 1 Procesador con 16 threads

La memora RAM BASE deberá ser cuando menos de:

- 32 GB de memoria RAM

Incremento de 1 GB de memoria RAM Servidores RISC.

El Instituto considera que durante la vigencia del contrato, por las necesidades naturales de la operación y evolución de sus aplicaciones, será necesario que en algunos servidores RISC se incremente la memoria RAM, por lo cual el proveedor establece un incremento de 1GB de memoria que oferta el Proveedor.

La Interface de red deberá incluir por lo menos:

- 8 puertos de red RJ45, velocidad 10 Gbps Ethernet.

El equipo deberá contar al menos con 2 fuentes internas de poder hot plug redundantes.

El equipo deberá contar al menos con 2 ventiladores internos.

El equipo deberá tener las siguientes características RAS:

- Discos Hot-plug
- Tarjetas PCIe Hot-plug
- Fuentes de Alimentación y Ventiladores redundantes hot-swap
- Comprobación y Corrección de errores y paridad de memoria
- Fácil sustitución de componentes
- Controladores de disco RAID 0 , 1 y 1E / 10 integrado
- Arquitectura de gestión de averías incluyendo Predictive Self Healing

Para la Administración remota el equipo deberá contar con tarjeta de administración remota que permita la administración del mismo en una interfaz de modo texto, incluso si el equipo está apagado.

El Sistema Operativo deberá ser compatible 100% con al menos alguna de las siguientes versiones de Sistema Operativo:

- Oracle Solaris 11.1
- Oracle Solaris 10 1/13 más actualización de parches

Soporte para Sistemas Operativos Guest:

- Oracle Solaris 11.1
- Oracle Solaris 10 1/13 *
- Oracle Solaris 10 8/11 *
- Oracle Solaris 10 9/10 *

ANEXOS

DIVISIÓN DE CONTRATOS

- AIX Versión 7.1 *
- AIX Versión 6.1 *
- HP-UX 11i v3 *

* Más actualización de parches

2.1.3.1.2. Servidor virtual X86 Modalidades M1, M2, M3 y M6

El Procesador deberá ser de al menos alguna de las siguientes familias:

- Intel® Xeon® Processor E7 v3 Family
  - Cache de 20MB a 45MB
  - Velocidad de 1.90GHz a 3.20GHz
- Intel® Xeon® Processor 7000 Sequence
  - Cache de 4MB a 24MB
  - Velocidad de 1.90GHz a 3.20GHz

Y deberá ser escalable con al menos incrementos de:

- Módulos de 1 Procesador con 8 threads

La memora RAM BASE deberá ser cuando menos de:

- 32 GB de memoria RAM

Incremento de 1 GB de memoria RAM Servidores X86

El Instituto considera que durante la vigencia del contrato, por las necesidades naturales de la operación y evolución de sus aplicaciones, será necesario que en algunos servidores X86 se incremente la memoria RAM, por lo cual el proveedor establece un incremento de 1GB de memoria que oferta el Proveedor.

El chasis deberá estar optimizado para rack (De 1 unidad de rack) y que cuente con los rieles y accesorios necesarios para conectarse a un rack de 42U.

El adaptador de bus del host (HBA) deberá tener al menos 4 tarjetas para:

- 2 para soporte a la SAN velocidad mínima 10 Gigabit Ethernet
- 2 para respaldo velocidad mínima 10 Gigabit Ethernet

La Interface de video deberá estar Integrada a la tarjeta madre.

La tarjeta de red deberá incluir por lo menos 4 puertos de red RJ45, velocidad 10 Gigabit Ethernet.

La Unidad de DVD-R / CD-RW deberá estar Incluido.

El Disco Duro deberá tener al menos 2 discos duros SAS de 500 GB de capacidad, velocidad mínima de 15000 rpm.

El servidor y los discos duros deben soportar la característica Hot Plug.

La fuente de poder deberá contar al menos con 2 fuentes internas de poder hot plug redundantes.

El sistema deberá incluir conexión eléctrica para conectores tipo NEMA 5-15R, a 127 volts y 60 Hz.

En caso de traer otro tipo de conector, el Proveedor deberá Implementar sin costo para el Instituto el tipo de conector eléctrico que requiera la solución que oferta.

Deberá incluir al menos un puerto de conexión al teclado, al mouse y otro al monitor.

Deberá incluir al menos 2 puertos USB libres sin considerar las conexiones de teclado y mouse.

Contar con password de arranque y password de setup de BIOS.

Deberá contar al menos con 2 ventiladores internos.

Deberá contar con tarjeta de administración remota que permita la administración del mismo en una interfaz de modo texto, incluso si el equipo está apagado.

El Sistema Operativo deberá ser compatible, entre otras, con las siguientes versiones de Sistema Operativo:

- Oracle Linux 5X, 6X o 7X
- Windows 2008 / 2012 / 2014 Server
- Diferentes Distribuciones Linux

Entorno para el usuario final

2.1.3.1.3. Puntos de Acceso a la Nube

Estación de trabajo cliente cero

- No incluye Sistema Operativo
- No incluye memoria RAM
- Alto desempeño, bajo consumo de energía
- Unidad DVD R/W
- Lector de Tarjetas Inteligentes integrados
- Puerto de red Ethernet
- Soporte para dos Monitores

- 6 Puertos USB
- Unidad DVD R/W integrado
- Mouse óptico de 2 botones
- Teclado en español
- Monitor de 19 pulgadas como mínimo

2.1.3.1.4. Escritorio en la Nube

Creación y configuración de un escritorio de trabajo que contenga:

- Instalación de sistema operativo
- Instalación de software base
- Creación de perfil de usuario
- Configuración

2.1.4. Virtualización

Plataforma de Virtualización

2.1.4.1.1. Plataforma de virtualización multi-tecnología

El Proveedor deberá suministrar una plataforma de virtualización que soporte las diferentes tecnologías de sistema operativo.

Debe incluir todo el software y hardware, así como licencias de software, instalación, configuración, puesta a punto, soporte, operación, administración y todo lo necesario para su correcta implementación.

Debe soportar la creación y administración de máquinas virtuales así como la configuración de toda la solución conforme a lo requerido por el Instituto.

El Instituto podrá solicitar durante la vigencia del contrato servicios de virtualización solicitados para las tecnologías que tenga establecidas el Instituto en el repositorio de arquitectura de la Nube IMSS.

Actividades que deberá realizar el Proveedor como parte del servicio de plataforma de virtualización:

- Instalación, Configuración y administración de la consola de administración para la plataforma de virtualización.
- Creación de nuevas máquinas virtuales que se necesiten por nuevas necesidades del Instituto.

- Configurar la solución de virtualización a efecto de proporcionar de manera temporal, dinámica y sin afectar ninguna de las máquinas virtuales involucradas, capacidad extra a una o más máquinas virtuales durante un intervalo de tiempo determinado con el fin de atender procesos que requieran ocasionalmente más recursos de procesamiento y/o memoria.
- Configurar la solución de virtualización a efecto de permitir mantenimiento a los equipos físicos, dándolos de baja de manera automatizada y transparente para el data center virtual, moviendo máquinas virtuales a otros nodos activos.
- Configurar la solución de virtualización a efecto de mantener un balanceo dinámico de los recursos de hardware asignados a una o más de las máquinas virtuales del Instituto, relocalizando máquinas virtuales en nodos con menor carga de trabajo sin sufrir afectación de ninguna clase en las mismas.
- Configurar la solución de virtualización a efecto de prevenir interrupciones en el servicio a causa de fallas de hardware, proporcionando un ambiente de alta disponibilidad en hardware que permita relocalizar de manera automática y sin afectación alguna en los servicios o procesos las máquinas virtuales del Instituto en uno o más nodos activos.
- Configurar la solución de virtualización para mover máquinas virtuales entre servidores físicos y/o sistemas de almacenamiento tipo SAN/FC, iSCSI y NFS sin la necesidad de apagar las máquinas virtuales, es decir, debe poder migrar máquinas virtuales entre máquinas físicas en línea y sin interrupción en la disponibilidad de las aplicaciones y servicios que residen sobre las máquinas virtuales.
- El software de Virtualización debe de tener la capacidad de utilizar switches distribuidos que existan a través de dos o más hosts que pertenezcan a un cluster y a su vez se administren de forma centralizada, además los switches distribuidos deben de cumplir con los siguiente:
  - Soporte de VLANs privadas
  - Soporte de L2 Forwarding
  - Soporte de IEEE 802.1Q VLAN Trunking
  - Soporte de VLAN Segmentation
- Configurar la solución de virtualización a efecto de realizar la virtualización de equipos físicos o la conversión de máquinas virtuales en formatos de una plataforma de virtualización a otra.
- Configurar la solución de virtualización a efecto de realizar la instalación y actualización al software de virtualización, empleando la consola central de administración como medio de envío (deployment) de dichas instalaciones y/o actualizaciones sin necesidad de interrumpir los servicios de las máquinas de virtuales.

Configurar la solución de virtualización a efecto de crear mensualmente, sin caer en interrupciones del servicio, imágenes de máquinas virtuales activas o inactivas a manera de respaldo o con el fin de mantener máquinas virtuales para probar actualizaciones o parches permitiendo analizar el comportamiento del sistema operativo o sus aplicaciones.

ANEXOS

DIVISIÓN DE CONTRATOS

2.2. Red

2.2.1. Zona

Punto Neutro

El Instituto requiere establecer comunicación desde diferentes ubicaciones o localidades remotas hacia el centro de datos ofertado, donde podrán converjer distintos carrier's. En este Punto Neutro tendrá que proporcionar a través de su infraestructura de red LAN el trasporte de datos, video y voz que se reciban de los distintos proveedores de enlaces de comunicación.

Punto Neutro será responsable de alojar la acometida del servicio de Internet con la que hoy cuenta el Instituto, a trves del cual se brindarán accesos a internet, para la consulta y transferencia de información, así como se hará la publicación de servicios WEB.

Características mínimas a cumplir en cuanto a capacidad, funcionalidad, operación y disponibilidad del punto neutro:

- Debera incluir Interfaces Fisicas redundantes, con infraestructura de Comunicaciones en Alta Disponibilidad tipo "carrier class" dedicada, con capacidad instalada para operar al menos lo siguiente:
  - 48 Interface Rj45 en cobre a velocidad de al menos 1 Gbps,
  - 48 Interface Ópticas a velocidad 1 o 10 Gbps.
  - 6 Clases de Servicio MPLS.
  - Infraestructura "Nonblocking".
  - Interconexión de componentes en Malla con enlaces de alta capacidad 40 y 100 Gbps.
  - Capacidad de conectar al menos 35 Redes MPLS.
  - Capacidad de conectar al menos 35 Enlaces Punto a Punto. (ruteables).
  - Capacidad de conectar al menos 35 Enlaces L2L.
  - Capacidad para recibir 1000 usuarios de VPN "site to site" en IPSEC de diferentes fabricantes de equipo.
  - Capacidad de recibir 1000 usuarios de VPN "cliente to site" en IPSEC con dispositivos móviles.
  - Monitoreo continuo de todos los componentes de esta solución así como de los servicios integrales de comunicaciones.
  - Acceso al centro de datos con trayectoria redundante diferentes, TIER 4.
  - Capacidad de interoperar protocolos ruteo de la Industria tales como OSPF, BGP4, entre otros, así como el uso de protocolo MPLS y IPV4, IPV6.
  - Crecimiento de anchos de Banda y escalabilidad en línea o sin disrupción.
  - Aplicación de QoS y VRFS para la capa de WAN.
  - Configuración "Multihoming" de al menos 10 proveedores de Internet con interfaces de 1 Gbps.

- Capacidad y Disponibilidad de interactuar en conjunto con otro proveedor de servicios para lograr automatizar la redundancia a las comunicaciones tanto en la capa de WAN como la de Internet.
- Las políticas de acceso físicas al Punto Neutro, serán las estipuladas por el Centro de Datos donde está alojada la Infraestructura del Instituto.

El Punto Neutro debe soportar recibir al menos los siguientes servicios:

- 1 Enlace redudante a Internet con un ancho de banda inicial de 1 Gbps y un máximo de 10 Gbps.
  - Deberá recibirse con Interfaces físicas necesarias en cobre (RJ45) u ópticas (MTRJ) compatibles con la velocidad al menos de 1 Gbps y de 10 Gbps.
  - En caso de requerirse en Punto Neutro uno o más tendidos nuevos o reubicaciones de cableado ya sea UTP o fibra óptica, deberá proporcionarse con cables categoría 6 y multimodo respectivamente, las Interfaces en cobre (RJ45) u ópticas (MTRJ) que soporten al menos la velocidad al menos de 1 Gbps y de 10 Gbps.
  - La Infraestructura de equipo de comunicaciones deberá proprocionarse en alta disponibilidad.
- 2 Enlaces LAN to LAN redudndantes con un ancho de banda inical de 200 Mbps y un máximo de 10 Gbps.
  - Deberá recibirse con Interfaces físicas necesarias en cobre (RJ45) u ópticas (MTRJ) compatibles con la velocidad al menos de 1 Gbps y de 10 Gbps.
  - En caso de requerirse en Punto Neutro uno o más tendidos nuevos o reubicaciones de cableado ya sea UTP o fibra óptica, deberá proporcionarse con cables categoría 6 y multimodo respectivamente, las Interfaces en cobre (RJ45) u ópticas (MTRJ) que soporten al menos la velocidad al menos de 1 Gbps y de 10 Gbps.
  - La Infraestructura de equipo de comunicaciones deberá proprocionarse en alta disponibilidad.
- 2 Enlaces MPLS redundantes con un ancho de banda inicial de 500 Mbps y un máximo de 10 Gbps.
  - Deberá recibirse con Interfaces físicas necesarias en cobre (RJ45) u ópticas (MTRJ) compatibles con la velocidad al menos de 1 Gbps y de 10 Gbps.
  - En caso de requerirse en Punto Neutro uno o más tendidos nuevos o reubicaciones de cableado ya sea UTP o fibra óptica, deberá proporcionarse con cables categoría 6 y multimodo respectivamente, las Interfaces en cobre (RJ45) u ópticas (MTRJ) que soporten al menos la velocidad al menos de 1 Gbps y de 10Gbps.
  - La Infraestructura de equipo de comunicaciones deberá proprocionarse en alta disponibilidad.
- 2 Enlaces MPLS redundantes con un ancho de banda inicial de 1 Gbps y un máximo de 10Gbps.
  - Deberá recibirse con Interfaces físicas necesarias en cobre (RJ45) u ópticas (MTRJ) compatibles con la velocidad al menos de 1Gbps y de 10Gbps.
  - En caso de requerirse en Punto Neutro uno o más tendidos nuevos o reubicaciones de cableado ya sea UTP o fibra óptica, deberá proporcionarse con cables categoría

6 y multimodo respectivamente, las Interfaces en cobre (RJ45) u ópticas (MTRJ) que soporten al menos la velocidad al menos de 1 Gbps y de 10Gbps.
  - La Infraestructura de equipo de comunicaciones deberá proprocionarse en alta disponibilidad.
- 1 Enlace MPLS redudndante con un ancho de banda de 10Mbps.
  - Deberá recibirse con Interfaces físicas necesarias en cobre (RJ45) u ópticas (MTRJ) compatibles con la velocidad al menos de 1Gbps y de 10Gbps.
  - En caso de requerirse en Punto Neutro uno o más tendidos nuevos o reubicaciones de cableado ya sea UTP o fibra óptica, deberá proporcionarse con cables categoría 6 y multimodo respectivamente, las Interfaces en cobre (RJ45) u ópticas (MTRJ) que soporten al menos la velocidad al menos de 1 Gbps y de 10Gbps.
  - La Infraestructura de equipo de comunicaciones deberá proprocionarse en alta disponibilidad.

El Punto Neutro debe incluir las siguientes características, funcionalidades y servicios.

Red de Área Amplia (WAN)

Para Punto Neutro la Red de Area Amplia debe de entenderse como la capacidad en la infraestructura, que permita recibir enlaces de Internet, así como del tipo LAN to LAN y MPLS descritos en el presente anexo.

El servicio de Red de Área Amplia deberá otorgar un medio de acceso confiable, donde de manera dedicada pueda transportar información que el Instituto tenga que transmitir entre los puntos que serán interconectados a través de los enlaces antes mencionados; toda vez que es indispensable contar con infraestructura de alta disponibilidad para el intercambio de información entre los sistemas críticos de la operación del Instituto. Cada acceso de Red de Área Amplia deberá considerar e incluir las siguientes características:

- Políticas de Enrutamiento (Policy Routing) para direccionar el tráfico según criterios establecidos, como son: la dirección origen del paquete, el tipo de trafico o cualquier otra información contenida en el paquete.
- Clase de Servicio (COS Class of Service), que permita identificar la clase del tráfico de datos, de video y/o de voz.
- Calidad de Servicio (QoS Quality of Service), que permita asignar colas de prioridad para garantizar la prioridad de aquellos paquetes sensibles al retardo (video y voz) de los que no lo son o de aplicaciones criticas.
- En caso de que el Instituto solicite un enlace con redundancia, los enlaces deberán poder operar n los siguientes esquemas:
  - Activo – Pasivo. En este tipo de esquema se encontrará uno enlace funcional (primario) y el otro estará disponible (respaldo o secundario) para que en caso de falla del primero, se conmute el tráfico hacia el de respaldo, con un tiempo de afectación mínimo. Se debe incluir además el transporte, la conmutación, así como el enrutamiento de paquetes, a conveniencia o solicitud del Instituto.

  - Activo – Activo. En este tipo de esquema ambos enlaces estarán disponibles para el trasporte de paquetes, en caso de falla de alguno de los dos el que quede disponible absorberá todo el tráfico, por lo que no existe tiempo de afectación; en estos enlaces se deberá balancear el tráfico. Se debe incluir además el transporte, la conmutación así como el enrutamiento de paquetes, a conveniencia o solicitud del Instituto.

Red de Área Local

Para Punto Neutro la Red de Área Local debe de entenderse como la capacidad en la infraestructura, que permita transportar los paquetes de datos, voz y video que se reciban de enlaces de Internet, LAN to LAN y MPLS (descritos en el presente anexo), redireccionandolos hacia los destinos correspondientes.

El Servicio de Red de Área Local en el Centro de Datos ofertado deberá considerar e incluir toda la infraestructura y los insumos necesarios para brindar conectividad a los diferentes dispositivos de TICS dentro de la Red LAN del Propio Centro de Datos así como a los dispositivos ubicados en las diferentes zonas desmilitarizadas que expondrán servicios web a Internet.

El Servicio deberá considerar e incluir toda la infraestructura y los insumos necesarios para brindar conectividad a las diferentes aplicaciones del Instituto y dispositivos de TICS que así lo requieran. Deberá contar con mecanismos de separación de tráfico para coadyuvar a una mejor administración de la infraestructura de TICS.

Deberá mantener una alta disponibilidad para el intercambio ágil, rápido íntegro y confiable de la información entre los servicios del Instituto que estarán conectados.

Las características mínimas a incluir son:

- El Posible Proveedor deberá crear al menos una VLAN para lograr la extensión del direccionamiento LAN del Instituto, sin embargo, el Instituto podrá solicitar la creación de VLAN's adicionales, en caso de que surja la necesidad de dividir o aislar tráfico de algunas aplicaciones o servicios.
- El Posible Proveedor deberá garantizar el flujo de tráfico entre todas las VLAN's que solicite el Instituto. Todas las VLAN's deberán ser implementadas con un ancho de banda de al menos 1 GB, por lo que el Proveedor deberá considerar el equipamiento necesario para lograrlo.
- El posible Proveedor deberá considera que todas las VLANs deberán estar debidamente aisladas de otros clientes que tengan servicios en el Centro de Datos contratado actualmente por el Instituto, de forma que ningún paquete de datos que fluya sobre la o las VLAN's que se implementen para el Instituto viaje a través una VLAN de otro cliente; tampoco estará permitido que paquetes de datos de otros clientes del Posible Proveedor viajen a través de las VLAN's que se implementen para el Instituto.

- El incumplimiento del aislamiento de las VLAN's por parte del Proveedor, se interpretará como un incumplimiento del servicio y una violación del acuerdo de confidencialidad que se solicita al Posible Proveedor, por lo que éste se hará acreedor a las sanciones correspondientes.
- El Posible Proveedor deberá considerar e incluir el transporte, la conmutación así como el enrutamiento de paquetes, a conveniencia o solicitud del Instituto.
- Debido a que los servicios de red son la base de operación de todo servicio de TIC que se proporcione al Instituto, cualquier falla en los servicios de red, se considerará como una falla en los servicios que soportan la operación del Instituto, afectando la disponibilidad de las aplicaciones involucradas, lo que originará las sanciones correspondientes
- Los servicios de red descritos no representarán costos adicionales para el Instituto, pues se entiende que forman parte del servicio cotizado en un periodo mensual unitariamente al Instituto.
- El Instituto requiere que la conectividad a nivel de red en tecnología, topología y protocolo Ethernet para el equipamiento, incluya todos los elementos de red pasivos con categoría 6 y los elementos de red activos; estos últimos con al menos redundancia en fuentes de poder y en su caso redundancia tarjetas controladoras o administradoras.
- El Instituto tiene el derecho de efectuar en cualquier momento y las veces que considere necesario, las inspecciones físicas en las instalaciones del Proveedor, con la finalidad de verificar el cumplimiento de lo solicitado.
- El Posible Proveedor deberá considerar e incluir la infraestructura necesaria para estar en condiciones de recibir enlaces con terceros de diferentes anchos de banda e incluso diferentes carrier's, por los cuales el instituto intercambia de manera segura información con diversas Instituciones.
- El Posible Proveedor deberá integrar todo lo necesario para soportar la recepción de enlaces LAN to LAN (L2L), para generar la conectividad con terceros.

Conectividad a Internet

Para Punto Neutro la Conectividad a Internet debe de entenderse como la capacidad en la infraestructura, que permita transportar los paquetes de datos, voz y video que se reciban de enlaces de Internet (conectividad hacia los servicios web nacionales y mundiales) con los que cuente el Instituto, redireccionandolos hacia los destinos correspondientes.

Deberá considerar e incluir todas las medidas de seguridad perimetral así como los componentes necesarios que brinden garantía técnica para que la información que curse a través de la infraestructura de Punto Neutro sea íntegra, confiable y disponible.

Deberá tener la flexibilidad para soportar crecimiento en Ancho de Banda en múltiplos de 100, 200 Mbps y 1Gbps hasta un máximo de 10Gbps.

Dentro de la infraestructura que brinde acceso al servicio de Internet se deberán considerar e integrar los siguientes elementos:

- 10 Interfaces Físicas en Rj45 en cobre a velocidad 1 Gbps.
- 10 Interfaces Ópticas con fibra a velocidad 1 o 10 Gbps.
- Infraestructura de Comunicaciones en Alta Disponibilidad.
- Direccionamiento IP Público IPV4, IPV6 homologado
- Capacidad de conectar Proveedores de Internet con capacidad de recibir todas las tablas de ruteo en el Internet en una interface de 1 Gbps.
- Monitoreo de Red y Abusos mediante un Noc y SOC respectivamente.
- Infraestructura dedicada.
- Administrar los recursos lógicos de IPV4, IPV6 y A.S de acuerdo a las instrucciones del Instituto.
- Administrar el filtrado de direcciones IP's a los Puntos Neutros con el fin de proteger la seguridad e integridad de los recursos lógicos del Instituto.
- Fomentar el uso e implementación del protocolo IPV6 para fines de mejora sobre los servicios del Instituto.
- Dispositivos de seguridad perimetral (firewall, IDP, IPS, etc.),
- Enlaces limpios (Clean Pipes),
- Filtrado de contenido en las consultas y descargas,
- ingeniería de tráfico que contemple la administración y modelado de ancho de banda en el medio de transmisión.

Deberá contar con el Monitoreo y seguimiento del direccionamiento homologado del IMSS.
Deberá generar reportes de capacidad de infraestructura de datos para el crecimiento con las menores afectaciones a la operación.

Conectividad a Intranet

Para Punto Neutro la Conectividad a Intranet debe de entenderse como la capacidad en la infraestructura, que permita transportar los paquetes de datos, voz y video que se reciban de los diferentes usuarios internos del Instituto, redireccionandolos hacia los destinos correspondientes.

El Servicio deberá considerar e incluir toda la infraestructura y los insumos necesarios para brindar conectividad a las diferentes aplicaciones del Instituto y dispositivos de TICS que así lo requieran.
Deberá contar con mecanismos de separación de tráfico para coadyuvar a una mejor administración de la infraestructura de TICS.

Deberá mantener una alta disponibilidad para el intercambio ágil, rápido íntegro y confiable de la información entre los servicios del Instituto que estarán conectados.

Las características mínimas a incluirse son:

- Se deberá crear al menos una VLAN para lograr la extensión del direccionamiento LAN del Instituto, sin embargo, el Instituto podrá solicitar la creación de VLAN's adicionales, en caso de que surja la necesidad de dividir o aislar tráfico de algunas aplicaciones o servicios.
- Se deberá garantizar técnicamente el correcto flujo de tráfico entre todas las VLAN's que solicite el Instituto. Todas las VLAN's deberán ser implementadas con un ancho de banda de al menos 1,000 Mbps, por lo que el Proveedor deberá considerar e incluir el equipamiento necesario para lograrlo.
- El incumplimiento del aislamiento de las VLAN's por parte del Proveedor, se interpretará como un incumplimiento del servicio y una violación del acuerdo de confidencialidad que se solicita al Posible Proveedor, por lo que éste se hará acreedor a las sanciones correspondientes.
- El Posible Proveedor deberá considerar e incluir el transporte, la conmutación así como el enrutamiento de paquetes, de manera eficaz y eficiente, a conveniencia o solicitud del Instituto.
- Debido a que los servicios de red son la base de operación de todo servicio de TIC que se proporcione al Instituto, cualquier falla en los servicios de red, se considerará como una falla en los servicios que soportan la operación del Instituto, afectando la disponibilidad de las aplicaciones involucradas, lo que originará las sanciones correspondientes.
- Los servicios de red descritos no representarán costos adicionales para el Instituto, pues se entiende que forman parte del servicio cotizado en un periodo mensual unitariamente al Instituto.
- El Instituto requiere que la conectividad a nivel de red en tecnología, topología y protocolo Ethernet para el equipamiento, incluya todos los elementos de red pasivos con categoría 6 y los elementos de red activos; estos últimos con al menos redundancia en fuentes de poder y en su caso redundancia tarjetas controladoras o administradoras.

El Instituto tiene el derecho de efectuar en cualquier momento y las veces que considere necesario, las inspecciones físicas en las instalaciones del Proveedor, con la finalidad de verificar el cumplimiento de lo solicitado.

Conectividad a Extranet

Para Punto Neutro la Conectividad a Extranet debe de entenderse como la capacidad en la infraestructura, que permita la conexión a través de redes privadas virtuales (VPN), para acceder a información que el Instituto defina y que se encuentre alojada en Punto Neutro.

El Instituto requiere establecer comunicación hacia un Portal Institucional desde diferentes ubicaciones o localidades remotas hacia el centro de datos ofertado, mediante accesos desde Internet, para la consulta y transferencia de información a través de un canal cifrado y seguro.

La infraestructura encargada de gestionar la comunicación deberá contar con las siguientes características especificadas en el numeral 2.1.4 Redes Privadas Virtuales – VPN (C2S – S2S) del Apéndice 5.Especificaciones técnicas de seguridad de la información.

Conectividad a Través de Redes Privadas Virtuales (VPN)

El Punto Neutro deberá contar con capacidad de infraestructura para proporcionar conectividad a través de redes privadas virtuales en los siguientes esquemas:

- Site to Site (S2S)
- Client to Site (C2S)
- Host to Host (H2H)

Pública

2.2.1.1.1. Conectividad de Enlaces

La Calidad de Servicio (Qos) deberá cumplirse de extremo a extremo a nivel de todo el enlace o la red, ya sean LAN to LAN o MPLS, incluyendo la tecnología de CPE y la nube de la RPV. La tecnología y protocolos para habilitar esta calidad de servicio deberán ser homogéneas de extremo a extremo en toda la infraestructura de comunicaciones que le sea necesaria al licitante para brindar el servicio. Esta calidad de servicio se deberá alcanzar implementando mecanismos de control de retardo y prioridad de tráfico que aseguren técnicamente y operativamente un trato homogéneo para las aplicaciones en todo el trayecto de los flujos.

Deberá ofertar una solución que identifique paquetes en tiempo real sensibles al retardo mediante protocolo estándar RTP o mecanismo equivalente o superior, garantizando los niveles de servicio y tener la capacidad de realizar compresión de los encabezados de paquetes con miras de optimizar la utilización de ancho de banda en cada sitio.
Los enlaces de comunicaciones hacia los diferentes nodos de la red serán parte de un servicio basado en la transmisión de información sobre el protocolo IP- que permite la implementación de redes privadas virtuales para comunicar a los diferentes puntos de una organización de manera segura y confiable, contando con la capacidad de diferenciar los tipos de información transmitida -como voz, datos y video- para proporcionar diferentes niveles de prioridad o tratamiento a cada uno de ellos (Quality of Service/Class of Service).

Para los inmuebles (ID) en los que no se especifique el uso de clases de servicio, no se requiere que se garantice técnica u operativamente el uso de ancho de banda para alguna clase de servicio en particular, en estos casos el IMSS podrá solicitar al Licitante Ganador durante la vigencia del contrato, el uso de clases de servicio, por lo que el proveedor de servicios ganador deberá habilitarla conforme a los niveles de servicio solicitados sin que represente un costo adicional al IMSS.

La separación de la información en clases de servicio proporciona los medios lógicos para manejar la información de tal forma que pueda preestablecerse un ancho de banda mínimo por clase, en caso de congestión. El Licitante Ganador en conjunto con el IMSS determinará, previo análisis de las aplicaciones y necesidades del negocio, el número de clases de servicio a usar y la clasificación de su información.

La separación del tipo de tráfico no sólo debe realizarse a nivel del análisis de valores de DSCP, direcciones IP fuente/destino y puertos TCP/UDP fuente/destino, sino también a través de un análisis más granular de los protocolos. Por ejemplo, puede separarse tráfico de HTTP por URL o host, distinguiendo aplicaciones Web prioritarias de las de Internet.
El servicio deberá poder darse a través de 2 tipos de enlaces

Enlace MPLS

El proveedor deberá brindar enlaces bajo demanda, con la tecnología MPLS (Multi-Protocol Label Switching), que solicite el Instituto, soportando realizar funciones tales como:

- VRF's "virtual routing and forwarding"
- 16 Interfaces Físicas redundantes. Interface RJ45 en cobre a velocidad 1 Gbps.
- 16 Interface Óptica con fibra a velocidad 1 o 10 Gbps.
- 6 Clases de Servicio MPLS.
- Infraestructura de Comunicaciones en Alta Disponibilidad (High Availability).
- Conexión al DRP, Activo Activo.
- Direccionamiento IP privado.
- Capacidad de conectarse a una nube de MPLS.
- Cuente con la infraestructura para el Monitoreo de los componentes del enlace MPLS.
- Infraestructura dedicada.
- Protocolos estándares de la Industria, ruteo estático, OSPF, BGP4.
- Capacidad y Disponibilidad de interactuar en conjunto con otro proveedor de servicios para lograr automatizar la redundancia en los inmuebles del Instituto y/o Puntos Neutros.
- Integrar y formar parte de un Consejo Técnico liderado por el Instituto donde se debatan y consensen las mejores soluciones tecnológicas para el beneficio de los servicios de TIC del Instituto.
- Ingeniería de tráfico o administración y modelado de ancho de banda, que permita asignar prioridades, garantizar ancho de banda específico (por aplicación, protocolo, horario IP, etc.) así como utilizar el ancho de banda de manera dinámica.
- Políticas de Enrutamiento (Policy Routing) para direccionar el tráfico según criterios establecidos, como: la dirección origen del paquete, el tipo de tráfico o cualquier otra información contenida en el paquete.
- Clase de Servicio (COS Class of Service), que permita identificar el tráfico de datos, de video y/o de voz.

- Calidad de Servicio (QoS Quality of Service), que permita asignar colas de prioridad para garantizar la prioridad de aquellos paquetes sensibles al retardo (video y voz) de los que no lo son.
- Mapa de Enrutamiento (Route Map), que permita la discriminación o desvío de tráfico específico, a través de listas de acceso o listas de prefijos.
- Restricción de tráfico por Listas de Acceso.
- El Posible Proveedor deberá contar con los medios que le permitan atender las solicitudes que formule el Instituto sobre enlaces MPLS, para que estos puedan operar bajo los siguiente tipos y características:
    - Activo – Pasivo. En el que un enlace se encontrará funcional (primario) y el otro estará disponible (respaldo o secundario) para que en caso de falla del primero, se conmute el tráfico hacia el de respaldo, con un tiempo de afectación mínimo. Se debe incluir además el transporte, la conmutación así como el enrutamiento de paquetes, a conveniencia o solicitud del Instituto.
    - Activo – Activo. En el ambos enlaces estarán disponibles para el trasporte de paquetes, en caso de falla de alguno de los dos el que quede disponible absorberá todo el tráfico, por lo que no existe tiempo de afectación; en estos enlaces se deberá balancear el tráfico. Se debe incluir además el transporte, la conmutación así como el enrutamiento de paquetes, a conveniencia o solicitud del Instituto.

Deberá tener la flexibilidad para soportar crecimiento o decremento en Ancho de Banda en múltiplos de 10, 20, 100, 200 Mbps y 1Gbps hasta un máximo de 10Gbps.

El servicio deberá incluir la infraestructura de hardware y software necesaria para poder proporcionar todas las funcionalidades arriba descritas y además deberá incluir la instalación, implementación, puesta a punto, administración, mantenimiento y soporte para el servicio y la infraestructura involucrada para su prestación.

Enlace LAN to LAN

El Proveedor a través del establecimiento e implementación de un Enlace LAN to LAN (L2L) deberá lograr una extensión del direccionamiento LAN del sitio del Instituto que se trate. Lo anterior con el fin de mantener el mismo dominio de "broadcast" mediante un enlace Ethernet. Las interfaces pueden ser ópticas o en Ethernet.

Las características que deben cubrir este servicio son:

- Interfaces físicas en cobre (RJ45) u ópticas (MTRJ) a velocidad al menos de 1 Gbps.
- Interface óptica con fibra Multimodo a velocidad al menos 1 Gbps y hasta 10 Gbps.
- Infraestructura de comunicaciones en alta disponibilidad.
- Conexión al DRP activo-activo.
- Direccionamiento IP privado con la validación del Instituto.

- Capacidad de conectar al menos 1 (un) enlace "Lan to Lan" en múltiplos de 10, 20, 100 y 200 Mbps, en el Ancho de Banda hasta un límite máximo de 10Gbps. Fácil crecimiento de anchos de banda y escalabilidad en línea o sin disrupción.
- Monitoreo de red y análisis de tráfico.
- Acceso al centro de datos con doble trayectoria.
- Niveles de servicio 99.90%.
- Infraestructura dedicada.
- El apego a las políticas de acceso físicas al Punto Neutro, serán las estipuladas por el Licitante Ganador en acuerdo con el Instituto.
- Los enlaces se deberán de recibir en una capa extra de seguridad por medio de un cluster de firewalls que permita realizar DMZ independientes por enlace con el fin de acotar mediante políticas de "firewall" los accesos por puertos TCP/IP a las aplicaciones de la contratante.
- El centro de operaciones de seguridad del Licitante Ganador, realizará actividades de administración de los sistemas de seguridad, incluyendo el soporte técnico, monitoreo, manejo de incidentes de seguridad y administración de la configuración (altas, bajas y cambios), en un horario permanente.

Deberá tener la flexibilidad para soportar crecimiento o decremento en Ancho de Banda en múltiplos de 10, 20, 100, 200 Mbps y 1Gbps hasta un máximo de 10 Gbps.

El servicio deberá incluir la infraestructura de hardware y software necesaria para poder proporcionar todas las funcionalidades arriba descritas y además deberá incluir la instalación, implementación, puesta a punto, administración, mantenimiento y soporte para el servicio y la infraestructura involucrada para su prestación.

2.2.2. Infraestructura de Red

Hardware y Software

2.2.2.1.1. Acelerador WAN

El licitante ganador deberá suministrar el servicio de Aceleración de la Red WAN, incluyendo su implementación, configuración, puesta a punto, monitoreo, administración, mantenimiento y soporte.

El objetivo de este servicio es optimizar el ancho de banda acelerando la transferencia de datos para mejorar la experiencia del usuario final en una red de área amplia (WAN).

La Aceleración de la Red WAN debe componerse de al menos los siguientes elementos o caracteristicas:

- La solución propuesta para este servicio por el Licitante, deberá ser capaz de acelerar el tiempo necesario para que la información fluya hacia un destino desde una fuente a través de la red WAN, mediante el uso de técnicas de compresión y deduplicación de datos, dichas técnicas deberán permitir reducir la cantidad de los datos que necesita ser transmitida.
- La solución propuesta debe de funcionar como un acelerador mediante el almacenamiento en caché de los archivos duplicados o partes de estos, para que puedan ser referenciados en vez de tener que enviar a través de la red WAN de nuevo.
- La solución propuesta debe ser capaz de trabajar con esquemas de un equipo dedicado en cada extremo del enlace WAN, con el fin de conectar sitios del IMSS hacia el centro de datos; adicionalmente debe soportar usuarios móviles o remotos del Instituto, por lo que debe de contar con clientes (software móvil del cliente) que actuarán como aparatos localizados, permitiendo que el equipo del usuario remoto pueda almacenar en caché los archivos duplicados y partes de archivos de forma local. Estos clientes móviles se conectarán a dispositivos de hardware de aceleración WAN propuesta.
- La solución ofertada deberá contar con la funcionalidad de distinguir entre los controladores de optimización WAN (WOC) y aceleradores WAN. El WOC debe ofrece compresión y almacenamiento en caché de disco, optimizando aún más el vínculo WAN que representa problemas conocidos con la red protocolos comunes. Debe entenderse como Optimización de Protocolo utilizados como sistema Common Internet File (CIFS), Microsoft Exchange, e incluso de TCP/IP, para eliminar la sobrecarga.
- La solución ofertada debe incluir controladores de entrega de aplicaciones (ADC) para conexiones y aplicaciones asimétricas, centrándose en la optimización de la experiencia del lado del servidor usando técnicas tales como Secure Sockets Layer (SSL) de descarga, el almacenamiento en caché estática, así como el balanceo de carga para mitigar los picos en el tráfico y mejorar la experiencia del usuario final.

2.2.2.1.2. Gestor de Optimización WAN

El licitante ganador deberá suministrar el servicio de Optimización de la Red WAN, incluyendo su implementación, configuración, puesta a punto, monitoreo, administración, mantenimiento y soporte.

El objetivo de este servicio es maximizar la eficiencia del flujo de datos a través de una red de área amplia (WAN), a través del uso de tecnologías y técnicas que permitan aumentar la velocidad de acceso a aplicaciones críticas e información del Instituto.

Deberá tener la capacidad de mitigar los problemas de saturación de red y de aplicaciones en la WAN para asegurar que el rendimiento de aplicaciones y la replicación de datos cumplan los requisitos de recuperación de desastres.

Deberá contar con un alto rendimiento y arquitectura escalable la cual pueda reducir drásticamente los tiempos de replicación de datos y permitir un uso más eficiente del ancho de banda existente.

Deberá cifrar y acelerar los datos para optimizar y encriptar las transferencias de datos entre los centros de datos.

La Optimización de la Red WAN debe componerse de al menos los siguientes elementos o características:

- Conformación de tráfico, en el que se prioriza el tráfico y ancho de banda que se asigna en consecuencia.
- Deduplicación de datos, lo que reduce la cantidad de los datos que deben ser enviados a través de una red WAN para aplicaciones como son: copias de seguridad remotas, replicación y recuperación de desastres.
- Compresión, que permita reducir el tamaño de los datos para limitar y así optimizar el uso de ancho de banda, ésta compresión debe ser adaptativa simétrica la cual deberá aplicar de forma automática el algoritmo de compresión apropiado para reducir drásticamente la cantidad de tráfico que tiene que ser enviado entre los centros de datos.
- Almacenamiento, que permita crear y mantener un caché de datos identificados con mayor frecuencia de utilización, para que estos estén alojados localmente para un acceso más rápido.
- Deberá reducir los efectos de latencia en aplicaciones que se ejecuten sobre la WAN mediante la optimización de los protocolos asociados a estas, incluyendo CIFS, MAPI, HTTP, entre otros
- Deberá contar con control del tráfico para gestionar y priorizar ancho de banda para aplicaciones específicas, asegurando que los usuarios que acceden a aplicaciones críticas a través de la WAN siempre reciban una respuesta rápida en las consultas que realicen.
- Control de la red para detectar el tráfico no esencial.
- Normas y Políticas para aplicarse a las descargas y el uso de Internet.
- Método para agrupar protocolos utilizados.
- Deberá mejorar el rendimiento de las aplicaciones acelerando la transferencia de datos a través de la WAN. Deberá acelerar la transferencia de grandes archivos, replicación de datos (para bases de datos, máquinas virtuales y Buzones de Microsoft Exchange), entre otros.
- La solución deberá ser a través de un dispositivo de uso específico que integre tanto el hardware como el software necesario.

Virtualización de redes

2.2.2.1.3. Balanceador de carga de capas L4-L7

Se requiere el suministro de servicios de Balanceo L4-L7 para aplicaciones Web o equivalente y su información inherente. La infraestructura propuesta deberá cumplir con las siguientes especificaciones técnicas mínimas.

- Ser por lo menos de alguna de las siguientes familias:
  - BIG-IP 7000 Series
  - BIG-IP 10000 Series
  - BIG-IP 12000 Series
  - Thunder CGN
  - Thunder ADC
  - AX ADC
- Soportar por lo menos alguno de los siguientes módulos:
  - Local Traffic Manager
  - Aceleración SSL
  - WAN Optimization Manager (WOM)
  - WAN Acceleration
  - Advanced Firewall Manager
  - Application Acceleration Manager
  - Server Load Balancing (SLB)
  - Global Server Load Balancing (GSLB)
  - Firewall Load Balancing (FWLB)
  - Carrier Grade NAT (CGNAT)
  - IPv6 Transition Technologies
  - Traffic Acceleration
  - SSL Offload
  - AFleX Scripting
  - aXAPI Custom Management
  - Multi-Tenancy/Virtualization
  - DDoS Protection
  - SSL Insight
  - Web Application Firewall
  - DNS Application Firewall
- Tener al menos 24M conexiones concurrentes L4 y Throughput: 19 Gbps/20 Gbps L4/L7

2.3. Instalaciones

2.3.1. Co-ubicación en modalidades de despliegue

Modalidades de despliegue

2.3.1.1.1. Nodo de Extensión de Nube Privada

Nodos de Extensión de Nube Privada (ENP) en los puntos con mayor demanda transaccional de operación de los servicios del Instituto.

ENP Tamaño Chico

Características técnicas diferenciadas para un ENP tamaño chico, adicionales a las definidas en el Anexo Técnico:

- 4 Racks de 5KW cada uno
- 2 CRACs en N+1
- UPS modular N+1, Carga Max. 20KW

ENP Tamaño Grande

Características técnicas diferenciadas para un ENP tamaño grande, adicionales a las definidas en el Anexo Técnico

- 8 Racks de 6.5KW cada uno
- 3 CRACs en N+1
- UPS modular al menos N+1, Carga Max 60KW

2.3.1.1.2. Nodo de Extensión de Nube Híbrida

Nodos de Extensión de la Nube Híbrida (ENH) del IMSS para persistencia y disponibilidad de servicios para usuarios externos a la Nube privada IMSS conforme a los especificado dentro del Anexo de Técnico.

Modalidades de co-ubicación

2.3.1.1.3. Piso Blanco

Se requiere contar con el servicio de metro cuadrado de piso blanco en las instalaciones del proveedor, con la finalidad de poder alojar equipamiento propio o de otros proveedores externos

en las instalaciones del proveedor y para lo cual debe contar con las especificaciones técnicas mínimas siguientes:

- Contar con las conexiones eléctricas necesarias para su operación.
- Contar con sistema de control del aire en los aspectos de ventilación, limpieza del aire, temperatura y humedad dentro de las instalaciones del site.
- Contar con la Seguridad física y lógica para el acceso a la ubicación del equipo y su información respectivamente.
- Redundancia eléctrica.
- Conexión con otros equipos ubicados en las instalaciones del proveedor u otras instalaciones indicados por el Instituto.

El Administrador del Contrato del Instituto designará al personal que podrá hacer las visitas y corroboraciones que considere pertinentes a las instalaciones del piso blanco durante la vigencia del contrato con el objeto de verificar la veracidad de la información proporcionada, las condiciones físicas y de operación.

2.3.1.1.1. Espacio en Rack

Se requiere contar con el servicio de unidades de espacio en Rack en las instalaciones del proveedor, con la finalidad de poder alojar equipamiento propio o de otros proveedores externos en las instalaciones del proveedor y para lo cual debe contar con las especificaciones técnicas mínimas siguientes:

- Contar con las conexiones eléctricas necesarias para su operación.
- Contar con sistema de control del aire en los aspectos de ventilación, limpieza del aire, temperatura y humedad dentro de las instalaciones del site.
- Contar con la Seguridad física y lógica para el acceso a la ubicación del equipo y su información respectivamente.
- Disponibilidad en rack.
- Redundancia eléctrica.
- Conexión con otros equipos ubicados en las instalaciones del proveedor u otras instalaciones indicados por el Instituto.
- Incluir el Piso Blanco.

El Administrador del Contrato del Instituto designará al personal que podrá hacer las visitas y corroboraciones que considere pertinentes a las instalaciones durante la vigencia del contrato con el objeto de verificar la veracidad de la información proporcionada, las condiciones físicas y de operación.

3. Aplicaciones

3.1. Sistemas

ANEXOS

DIVISIÓN DE CONTRATOS

3.1.1. Gestión de recursos

Gestión de identidades

3.1.1.1.1. Open AM

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Open AM o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de Open AM edición o equivalente ForgeRock Subscription (soporte empresarial que incluye Indemnización legal)
- Versión del producto 10.0.0 y posteriores.
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.1.1.1.2. Oracle IDM

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Oracle IDM o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Subscripción de Oracle IDM (11g o superior) o equivalente (soporte empresarial 7/24 remoto y presencial con el mismo nivel de servicio que el Centro de Datos).
- Aplicación de actualizaciones y parches (releases/bugfixes).
- Acceso a base de conocimientos del fabricante.
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

3.1.1.1.3. NetIQ Access Manager Appliance (Access Gateway)

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma NetIQ o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de NetIQ Access Manager edición Appliance o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 4.1 y posteriores.
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2. Componentes de Aplicación

3.2.1. Análisis, reporteo y estadísticas

Reportes a la medida (Ad-hoc)

3.2.1.1.1. Microsoft Reporting Services

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Microsoft Reporting Services o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de Microsoft Reporting Services o equivalente (soporte empresarial)
- Versión estable y actual del producto
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.1.1.2. ESSBase

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma ESSBase o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de ESSBase o equivalente (soporte empresarial)
- Versión 11g y posteriores del producto
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto

- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.1.1.3. Hyperion

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Hyperion o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Hyperion o equivalente (soporte empresarial)
- Versión 9.3 y posteriores del producto
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

Inteligencia de negocio

3.2.1.1.4. Visualización y Analisis de Información

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Analitica y de Visualización de Información o equivalente según sus necesidades.

El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Analítica y de Visualización de Información o equivalente (soporte empresarial)
- Versión estable y actual del producto
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.1.1.5. Oracle Business Intelligence

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Oracle Business Intelligence Enterprise Edition o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de esta plataforma.

Requerimientos Mínimos

- Subscripción de soporte de Oracle Business Intelligence Enterprise Edition (11g o superior) o equivalente (soporte empresarial 7/24 en línea y presencial con el mismo nivel de servicio que el Centro de Datos)
- Aplicación de actualizaciones y parches (releases/bugfixes)
- Acceso a base de conocimientos del fabricante
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

3.2.1.1.6. Microsoft Analisys Services

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Microsoft Analisys Services o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Microsoft Analisys Services o equivalente (soporte empresarial)
- Versión 2014 y posteriores del producto
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.1.1.7. SAS

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma SAS o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de SAS o equivalente (soporte empresarial)
- Version 9.4 y posteriores del producto
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.1.1.8. Oracle Exalytics In-Memory Machine

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Oracle Exalytics In-Memory Machine o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Oracle Exalytics In-Memory Machine (en su versión más reciente) o equivalente (soporte empresarial 7/24 en línea y presencial con el mismo nivel de servicio del Centro de Datos)
- Aplicación de actualizaciones y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

Soporte a la toma de decisiones

3.2.1.1.9. Tableau Server

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Tableau Server o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Tableau Server o equivalente (soporte empresarial)
- Versión 10 y posteriores del producto
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.1.1.10. Tableau Desktop

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Tableau Desktop o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de Tableau Desktop o equivalente (soporte empresarial)
- Versión 10 y posteriores del producto
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

Análisis estadístico

3.2.1.1.11. Stata

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Stata o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Stata o equivalente (soporte empresarial)
- Versión 13 y posteriores del producto
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.2. Gestión de datos

Extracción, transformación y carga de datos (ETL)

3.2.2.1.1. Oracle ODI

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Oracle ODI o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Subscripción de soporte de Oracle ODI General Support (11g o superior) o equivalente (soporte empresarial 7/24 en línea y presencial con el mismo nivel de servicio del Centro de Datos)
- Aplicación de actualizaciones y parches (releases/bugfixes)
- Acceso a bases de conocimiento del fabricante

- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

3.2.2.1.2. IBM Data Stage

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma IBM DATA STAGE o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de IBM DATA STAGE Support o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 5.1 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.2.1.3. Microsoft Integrator Services

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Microsoft Integration Services o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Microsoft Integration Services Software Assurance o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 2008 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.2.1.4. Oracle Warehouse Builder

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Oracle Warehouse Builder o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Oracle Warehouse Builder General Support (11g o superior) o equivalente (soporte empresarial 7/24 en línea y presencial con el mismo nivel de servicio que el Centro de Datos)
- Aplicación de actualizaciones y parches (releases/bugfixes)
- Acceso a bases de conocimiento del fabricante
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

3.2.2.1.5. Integración y Transformación de Información

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma de Integración y Transformación de Información o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Integración y Transformación de Información o equivalente (soporte empresarial)
- Versión estable y actual del producto
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.2.1.6. Redbrick

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Stata Transfer o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Stata Transfer o equivalente (soporte empresarial)
- Versión del producto 12 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.2.1.7. Stata Transfer

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Redbrick o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Softwar de Redbrick o equivalente (soporte empresarial)
- Versión del producto 6.2 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

Integración e intercambio de datos

Gestión de la calidad de los datos

3.2.2.1.8. Oracle Data Quality

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Oracle DATA QUALITY o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Subscripción de soporte de Oracle DATA QUALITY 811g o superior) General Support o equivalente (soporte empresarial 7/24 en línea o presencial con el mismo nivel de servicios del Centro de Datos)
- Aplicación de actualizaciones y parches (releases/bugfixes)
- Acceso a bases de conocimiento del fabricante
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

Sistema de gestión de bases de datos

3.2.2.1.9. Bases de Datos Oracle

El Instituto podrá solicitar al proveedor la instalación del motor de Base de Datos Oracle de al menos las siguientes versiones: 10g release 2 o superior o equivalente. Esta instalación deberá incluir el licenciamiento que hoy en día usa el Instituto, así como el soporte y mantenimiento del producto najo un esquema 7/24 en line y presencial.

Para la entrega de la Plataforma e Infraestructura de Bases de Datos ORACLE o equivalente, el proveedor deberá realizar entre otras, las siguientes actividades:

- Instalar motores según las necesidades del Instituto, las cuales incluyen por lo menos:
  - StandAlone
  - RAC
- Crear, modificar y eliminar ambientes (Productivos, QA y Desarrollo) de acuerdo a los requerimientos que el Instituto determine (ASM, Filesystem), reutilizando el hardware asignado a estos ambientes para los fines que al Instituto convengan.
- Evaluar el hardware para el servidor de base de datos con la finalidad de verificar compatibilidad y garantizar que el producto pueda utilizar mejor los recursos informáticos disponibles como unidades de disco para los productos de Oracle, unidades de cinta dedicados disponibles, memoria disponible para las instancias de base de datos, entre otros.
- Planear la estructura de almacenamiento lógico de la base de datos, el diseño general de la base de datos, la estrategia de la copia de seguridad, el rendimiento del servidor de base de datos y de la misma base de datos, durante las operaciones de acceso a datos, la eficiencia de los procedimientos de respaldo y recuperación, la planificación del diseño relacional de los objetos de la base y las características de almacenamiento para cada uno de estos objetos, mediante la planificación de la relación entre cada uno y su almacenamiento físico antes de crearlo.
- Habilitar la base de datos para el correcto uso de los sistemas asociados (creación de servicios, usuarios, sinónimos, permisos, privilegios, entre otros).
- Implementar el diseño planeado sobre la estructura de almacenamiento lógico de la base de datos creando tablespaces y objetos de base de datos.
- Realizar cargas de información solicitada y autorizada por el Instituto en la misma o en otra instancia de base de datos.
- Descargar e instalar los parches previa autorización del instituto. Después de la instalación y de forma regular, descargar e instalar los parches. Los parches están disponible como parches provisionales individuales y como conjuntos de parches
- Acceso a bases de conocimiento del fabricante
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

3.2.2.1.10. Microsoft SQL Server

El Instituto podrá solicitar al proveedor la instalación del Motor de Base de Datos Microsoft o equivalente de al menos las siguientes versiones: 2008 SP1 o superior.

Este servicio incluirá el licenciamiento del producto y deberá incluir el soporte y mantenimiento del producto.

Para la entrega de la Plataforma e Infraestructura de Bases de Datos Microsoft o equivalente, el proveedor deberá realizar entre otras, las siguientes actividades:

- Instalar motores según las necesidades del Instituto.
- Crear, modificar y eliminar ambientes (Productivos, QA y Desarrollo) de acuerdo a las especificaciones que el Instituto determine (Unidades de Directorio).
- Evaluar el hardware para el servidor de base de datos con la finalidad verificar compatibilidad y garantizar que el producto pueda utilizar mejor los recursos informáticos disponibles como por lo menos unidades de disco para los productos de Microsoft, unidades de cinta dedicados disponibles , memoria disponible para las instancias de base de datos.
- Planear la estructura de almacenamiento lógico de la base de datos, el diseño general de la base de datos, la estrategia de la copia de seguridad, el rendimiento del servidor de base de datos y de la misma base de datos, durante las operaciones de acceso a datos, la eficiencia de los procedimientos de respaldo y recuperación, la planificación del diseño relacional de los objetos de la base y las características de almacenamiento para cada uno de estos objetos, mediante la planificación de la relación entre cada uno y su almacenamiento físico antes de crearlo.
- Abrir la base de datos en modo normal después de haberla diseñado.
- Crear y otorgar privilegios a usuarios y roles en la base de datos.
- Implementar el diseño planeado sobre la estructura de almacenamiento lógico de la base de datos creando tablespaces y objetos de base de datos.
- Implantar la base de datos en servidores adicionales, después de que haya una instalación de base de datos Oracle correctamente configurada, afinada, parcheada y probada, es posible que el Instituto desee implantar configuraciones de instalación similares a otros servidores, como pueden ser: múltiples sistemas de bases de datos de producción. y/o Crear sistemas de desarrollo y pruebas que son idénticos a su sistema de producción.
- Realizar cargas de información solicitada y autorizada por el Instituto.
- Descargar e instalar los parches previa autorización del instituto. Después de la instalación y de forma regular, descargar e instalar los parches. Los parches están disponible como parches provisionales individuales y como conjuntos de parches.

3.2.2.1.11. DB2

El Instituto podrá solicitar al proveedor la instalación del Motor de Base de Datos DB2 o equivalente de al menos las siguientes versiones 7, 8 y 9.1

Este servicio incluirá el licenciamiento del producto y deberá incluir el soporte y mantenimiento del producto.

Para la entrega de la Plataforma e Infraestructura de Bases de Datos DB2 o equivalente, el proveedor deberá realizar entre otras, las siguientes actividades:

- Instalar motores de acorde a lo solicitado por el comité de arquitectura y/o de acuerdo a las necesidades que el Instituto requiera.
- Crear, modificar y eliminar ambientes (Productivos, QA y Desarrollo) de acuerdo a las especificaciones que el Instituto determine (Unidades de Directorio).
- Evaluar el hardware para el servidor de base de datos con la finalidad verificar compatibilidad y garantizar que el producto pueda utilizar mejor los recursos informáticos disponibles como por lo menos unidades de disco para los productos de DB2, unidades de cinta dedicados disponibles para los productos de, memoria disponible para las instancias de base de datos .
- Planear la estructura de almacenamiento lógico de la base de datos, el diseño general de la base de datos, la estrategia de la copia de seguridad, el rendimiento del servidor de base de datos y de la misma base de datos, durante las operaciones de acceso a datos, la eficiencia de los procedimientos de respaldo y recuperación, la planificación del diseño relacional de los objetos de la base y las características de almacenamiento para cada uno de estos objetos, mediante la planificación de la relación entre cada uno y su almacenamiento físico antes de crearlo.
- Abrir la base de datos en modo normal después de haberla diseñado.
- Crear y otorgar privilegios a usuarios y roles en la base de datos.
- Implementar el diseño planeado sobre la estructura de almacenamiento lógico de la base de datos creando tablespaces y objetos de base de datos.
- Implantar la base de datos en servidores adicionales, después de que haya una instalación de base de datos Oracle correctamente configurada, afinada, parcheada y probada, es posible que el Instituto desee implantar configuraciones de instalación similares a otros servidores, como pueden ser: múltiples sistemas de bases de datos de producción. y/o Crear sistemas de desarrollo y pruebas que son idénticos a su sistema de producción.
- Realizar cargas de información solicitada y autorizada por el Instituto.
- Descargar e instalar los parches previa autorización del instituto. Después de la instalación y de forma regular, descargar e instalar los parches. Los parches están disponible como parches provisionales individuales y como conjuntos de parches.

3.2.2.1.12. Subscripciones a Bases de Datos Open Source

El Instituto podrá solicitar al proveedor la suscripción al uso de Bases de Datos Open Source.

Este servicio incluirá el soporte y mantenimiento del producto.

Para la entrega de la Plataforma e Infraestructura de Bases de Datos OpenSource, el proveedor deberá realizar entre otras, las siguientes actividades:

- Instalar motores con la versión de acorde a lo solicitado por el comité de arquitectura y de acuerdo a las necesidades que el Instituto requiera.
- El proveedor deberá considerar al menos las siguientes plataformas de Base de Datos opencource: PostgreSQL, MySQL, Maria DB, Red Hat DB, Berkley DB, Cassandra DB, etc.
- Crear, modificar y eliminar ambientes (Productivos, QA y Desarrollo) de acuerdo a las especificaciones que el Instituto determine (Unidades de Directorio).
- Evaluar el hardware para el servidor de base de datos con la finalidad verificar compatibilidad y garantizar que el producto pueda utilizar mejor los recursos informáticos disponibles como por lo menos unidades de disco para los productos de OpenSource, unidades de cinta dedicados disponibles, memoria disponible para las instancias de base de datos.
- Planear la estructura de almacenamiento lógico de la base de datos, el diseño general de la base de datos, la estrategia de la copia de seguridad, el rendimiento del servidor de base de datos y de la misma base de datos, durante las operaciones de acceso a datos, la eficiencia de los procedimientos de respaldo y recuperación, la planificación del diseño relacional de los objetos de la base y las características de almacenamiento para cada uno de estos objetos, mediante la planificación de la relación entre cada uno y su almacenamiento físico antes de crearlo.
- Abrir la base de datos en modo normal después de haberla diseñado.
- Crear y otorgar privilegios a usuarios y roles en la base de datos.
- Implementar el diseño planeado sobre la estructura de almacenamiento lógico de la base de datos creando tablespaces y objetos de base de datos.
- Implantar la base de datos en servidores adicionales, después de que haya una instalación de base de datos Oracle correctamente configurada, afinada, parcheada y probada, es posible que el Instituto desee implantar configuraciones de instalación similares a otros servidores, como pueden ser: múltiples sistemas de bases de datos de producción. y/o Crear sistemas de desarrollo y pruebas que son idénticos a su sistema de producción.
- Realizar cargas de información solicitada y autorizada por el Instituto.
- Descargar e instalar los parches previa autorización del instituto. Después de la instalación y de forma regular, descargar e instalar los parches. Los parches están disponible como parches provisionales individuales y como conjuntos de parches.

3.2.2.1.13. Oracle Exadata Storage Expansion

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Oracle Exadata Storage Expansion o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Subscripción de soporte de Oracle Exadata Storage Expansion (en su versión más reciente) o equivalente (soporte empresarial 7/24 en línea o presencial con el mismo nivel de servicio que el Centro de Datos)
- en las instalaciones del Instituto
- Aplicación de actualizaciones y parches (releases/bugfixes)
- Acceso a bases de conocimiento del fabricante
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

3.2.2.1.14. SQL Server Parallel Data Warehouse

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma SQL Server Parallel Data Warehouse o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de SQL Server Parallel Data Warehouse o equivalente (soporte empresarial)
- Versión actual y posteriores del producto
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

Directorio

3.2.2.1.15. Open DJ

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Open DJ o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de Open DJ edición ForgeRock Subscription o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 2.4 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.2.1.16. NetIQ Access Manager (Identity Provider)

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma NetIQ o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de NetIQ edición standalone o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 4.1 y posteriores.
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.2.1.17. Plataforma LDAP

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma LDAP según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de LDAP (soporte empresarial)
- Versión estable y actual del producto.
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.3. Herramientas y entorno de desarrollo

Entorno de desarrollo integrado (IDE)

3.2.3.1.1. Team Foundation Server

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Team Foundation Server o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Team Foundation Server Software Assurance o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 10.0.0 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

Kit de Desarrollo de Software (SDK)

3.2.3.1.2. Java Development Kit

El Instituto podrá solicitar durante la vigencia del contrato los servicios de instalación y parametrización de la plataforma JAVA de acuerdo a las necesidades que se indiquen. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de JAVA
- Versión 1.4 o posterior del producto.
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.3.1.3. Java Enterprise Edition

El Instituto podrá solicitar durante la vigencia del contrato los servicios de instalación y parametrización de la plataforma JAVA de acuerdo a las necesidades que se indiquen. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de JAVA
- Version 1.4 o posterior del producto.
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.3.1.4. Java Runtime Environment

El Instituto podrá solicitar durante la vigencia del contrato los servicios de instalación y parametrización de la plataforma JAVA de acuerdo a las necesidades que se indiquen. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de JAVA
- Versión 1.4 o posterior del producto.
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.3.1.5. .NET Framework

El Instituto podrá solicitar durante la vigencia del contrato los servicios de instalación y parametrización de la plataforma .NET de acuerdo a las necesidades que se indiquen. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de .NET
- Versión 1.1 o posterior del producto.
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.4. Gestión de documentos y contenidos

Gestión de contenidos Web

3.2.4.1.1. Drupal

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Content Management DRUPAL o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de DRUPAL Support o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 7.0 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.4.1.2. Liferay Enterprise

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Content Management LIFERAY ENTERPRISE o equivalente según sus necesidades.

El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de Content Management LIFERAY ENTERPRISE Support o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 6.0 y posteriores
- Soporte del producto por el fabricante 5/8 o 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.4.1.3. Adobe ColdFusion

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma ADOBE COLD FUSION o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

- Software de ADOBE COLD FUSION Support o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 9.0 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.5. Middleware

Bus de servicios empresariales (ESB)

3.2.5.1.1. Oracle Service Bus

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Oracle Service Bus o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Subscripción de soporte de Oracle Service Bus General Support (11g o superior) o equivalente (soporte empresarial 7/24 en línea o presencial con el mismo nivel de servicio que el Centro de Datos)
- Aplicación de actualizaciones y parches (releases/bugfixes)
- Acceso a bases de conocimiento del fabricante
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO
HOJA 66 DE 89
Formato SGMP F03
VERSIÓN 5.0
Apéndice #1. Bloques de Construcción Fundamentales

3.2.5.1.2. SOA Suite

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Oracle SOA Suite o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Subscripción de soporte de Oracle SOA Suite General Support (11g o posterior) o equivalente (soporte empresarial 7/24 en línea y presencial con el mismo nivel de servicio que el Centro de Datos)
- Aplicación de actualizaciones y parches (releases/bugfixes)
- Acceso a bases de conocimiento del fabricante
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

Software de mensajería

3.2.5.1.3. Apache Kafka

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Apache Kafka o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de Apache Kafka Support o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 0.8 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

Servidores de Aplicaciones

3.2.5.1.4. WebLogic

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Oracle WEBLOGIC o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Subscripción de soporte de Oracle WEBLOGIC General Support (8.1 o superior) o equivalente (soporte empresarial 7/24 en línea o presencial con el mismo nivel de servicio que el Centro de Datos)
- Aplicación de actualizaciones y parches (releases/bugfixes)
- Acceso a bases de conocimiento del fabricante
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

3.2.5.1.5. Tuxedo

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma TUXEDO o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de TUXEDO Support o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 9.2 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.5.1.6. GlassFish

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma GLASSFISH o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de GLASSFISH Support o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 2.0 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.5.1.7. Apache Tomcat

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Apache Tomcat o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de Apache Tomcat Support o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 2.0 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.5.1.8. Apache HTTPD

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Apache HTTPD o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de Apache HTTPD Support o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 2.0 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.5.1.9. Oracle Exalogic

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Oracle Exalogic o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Subscripción de soporte de Oracle Exalogic (en su versión más reciente) o equivalente (soporte empresarial 7/24 en línea y presencial con el mismo nivel de servicio del Centro de Datos)
- Aplicación de actualizaciones y parches (releases/bugfixes)

- Acceso a bases de conocimiento del fabricante
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

3.2.6. Automatización y gestión de procesos

Gestión de procesos de negocios (BPMS)

3.2.6.1.1. Oracle BPM

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Oracle BPM o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Subscripción de soporte de Oracle BPM (en su versión más reciente) o equivalente (soporte empresarial 7/24 en línea y presencial con el mismo nivel de servicio del Centro de Datos)
- Aplicación de actualizaciones y parches (releases/bugfixes)
- Acceso a bases de conocimiento del fabricante
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

Gestión de reglas de negocio

3.2.6.1.2. Motor de Reglas

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de las Herramientas de Gestión de Reglas de Negocio según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de Herramientas de Gestión de Reglas de Negocio (soporte empresarial)
- Versión estable y actual del producto.
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.2.7. Comunicación unificada y colaboración

Correo electrónico

3.2.7.1.1. Servicio de Correo Electrónico.

Se requiere el servicio de la administración del correo electrónico corporativo durante la vigencia del contrato.
Los requisitos mínimos que el proveedor deberá considerar son:

Configuración del Servicio:

- Contar con equipos de tecnología reciente y que los elementos de hardware que proponga deberán contar al menos con características redundantes como lo pueden ser:
  - Fuentes de poder
  - Procesadores
  - Discos duros
- Configurar la solución de correo en un esquema de Back-end y Front-end Server
- Establecer un esquema de optimización del correo que considere de manera enunciativa más no limitativa tareas como: desfragmentación de la base de datos del correo, revisiones de integridad de la base de datos del correo; depuraciones de logs del sistema operativo, servidores y de las soluciones diversas de antivirus antispam, antipishing, etc.
- Configurar el servicio de correo para habilitar el servicio de POP3 y SMTP.
- Configurar el servicio de correo para habilitar el acceso vía WebMail.
- Personalizar la página de entrada y de salida de la interface WebMail de acuerdo con los estándares que le defina el Instituto.
- Configurar el acceso para que permita a los usuarios conectarse a su buzón desde un Cliente de Correo. La interrupción en el servicio en los clientes será considerada como falla en el servicio de correo, por lo que se aplicará la deducción correspondiente de acuerdo a los Niveles de Servicio definidos.
- Configurar el servicio de correo para conexiones desde dispositivos móviles tales como: IOS, Android, Windows phone, BlackBerry.
- Inicialmente el Proveedor debe instalar el certificado de seguridad con el que cuenta el Instituto; en caso de que el Instituto no cuente con el mismo o una vez que la vigencia del certificado caduque, el Proveedor deberá adquirir, implementar y configurar dentro del servidor un certificado SSL a 256 bits y deberá estar ligado al nombre DNS del correo; estas características se deben de conservar durante la vigencia del contrato.
- Considerar inicialmente 82,000 cuentas de correo con al menos los siguientes perfiles para el tamaño de los buzones:

ANEXOS

DIVISIÓN DE CONTRATOS

Operativos	10	80
Operativos	20	5
Operativos	50	5
Divisionales	100	7
Coordinadores Normativos	500	2
Directores	10,000	1

- Trabajar en conjunto con el Instituto, las adecuaciones de las configuraciones del servicio de correo, como lo pueden ser: Número máximo de destinatarios, tamaño máximo de mensaje y lo que aplique.
- Hacer las configuraciones e instalaciones necesarias por solicitud del Instituto para integración con aplicaciones que utilice este servicio, como lo pueden ser (herramientas de colaboración). Estas aplicaciones son suministradas, administradas y operadas por personal del Instituto.

La falla en el servicio WebMail será considerada como incumplimiento en el servicio de correo, por lo que se aplicará la deducción correspondiente de acuerdo a los Niveles de Servicio definidos.

Filtrado de contenido:

El Proveedor deberá mantener el saneamiento del servicio de correo electrónico corporativo, por lo que la solución propuesta debe contar con software de antivirus licenciado tanto a nivel sistema operativo como a nivel aplicativo; el licenciamiento de este software deberá ser suministrado por el Proveedor. Así mismo, el proveedor deberá:

- Configurar herramientas de antivirus para que se realicen escaneos diarios del sistema operativo y de los buzones.
- Programar una tarea para que las definiciones de datos de la solución del antivirus se actualicen diariamente.
- Administrar de la solución de antivirus y tenerlo configurado con las mejores prácticas de administración que de manera enunciativa más no limitativa pueden ser: revisión en tiempo real, revisión de sector de arranque y memoria, revisión de archivos comprimidos, análisis heurístico, limpieza automática, zonas de cuarentena, escaneo de scripts, etc.
- Actualizar constantemente bloqueos por subjects y por archivos incrustados, tomando como base los boletines técnicos de los virus más recientes, previa validación y autorización del Instituto.

La solución propuesta debe contar con software para protección de males de la Web como son, al menos, el Phishing, el Spam y los Malwares, esta solución debe ser tanto a nivel sistema operativo como a nivel aplicativo, por lo que el proveedor deberá:

- Contar con herramientas, para cumplir con el requerimiento anterior; la solución puede ser de hardware o de software según lo decida el Proveedor.
- Gestionar la administración de la herramienta de acuerdo a las mejores prácticas de administración que de manera enunciativa más no limitativa pueden ser:
  - Actualizar de la base de datos antispam de acuerdo a las listas negras existentes en la Web.
  - Actualizar diariamente de dicha base de datos.
  - Configurar las reglas de entrada y de salida.
  - Bloquear de videos, música y/o imágenes.
  - Bloquear lenguaje pornográfico y/o alto contenido sexual.
  - Bloquear correos hacia cuentas inexistentes, etc.

Lo anterior previa validación y autorización del Instituto.
Las actualizaciones de la protección de Phishing, spam, malware e incluso el antivirus debe realizarse diariamente.

Respaldos y Restauración de la Información

El Proveedor deberá establecer un esquema de respaldos en línea y restauración de los buzones y bases de datos con los siguientes requerimientos:

- Considerar el respaldo total del buzón.
- El respaldo debe hacerse con periodicidad diaria, semanal y mensual.
- Los respaldos diarios tendrán un reciclaje de 7 días, los semanales de 4 semanas y los mensuales de 1 año.
- Realizarse en medios magnéticos u otro medio que sea externo al servidor.
- Conservar los respaldos semanales y mensuales en una bóveda externa, de modo que los únicos respaldos que podrán permanecer en el centro de datos primario serán los diarios.
- La restauración debe poder hacerse por buzón e incluso la base de datos de correo completa.
- La restauración no debe encimar o sobrescribir información que en esos momentos esté activa en el buzón en cuestión y por consiguiente deberá permitir al usuario copiar de forma personalizada la información recuperada. Por ejemplo, si se restaura la bandeja de elementos enviados, ésta no debe sobrescribir a la que está en producción, se espera que se genere una carpeta secundaria donde el usuario pueda hacer una selección de los mensajes que necesita.
- El Proveedor debe proporcionar el licenciamiento necesario en el software de respaldos para lograr el respaldo en línea

Seguridad y Vulnerabilidad

- El Proveedor deberá establecer un esquema de seguridad que proteja los bienes involucrados en la solución del servicio de correo, por lo que debe considerar al menos lo siguiente:
- Establecer un procedimiento de análisis de vulnerabilidades con base en herramientas comerciales que permita identificar si la solución ofertada está libre de vulnerabilidades conocidas; se deberá entregar un reporte al menos trimestral de dicho análisis.
- Tener la solución ofertada 100% libre de vulnerabilidades conocidas. En caso de que el servicio ofertado sea objeto de un ataque exitoso se aplicarán las deducciones correspondientes.
- Suministrar y utilizar sus propias herramientas de análisis de vulnerabilidades para cumplir con lo solicitado en el presente Anexo Técnico. Éstas no necesariamente deben de ser las mismas con las que cuenta el Instituto.
- El Instituto puede en cualquier momento ejecutar con sus propias herramientas para el análisis de vulnerabilidades (Con las que cuente el área de seguridad informática del Instituto en ese momento), en caso de detección de éstas, el Proveedor estará obligado a solucionarlas en un plazo no mayor a 3 días. No necesariamente por cada análisis del Proveedor habrá un análisis del Instituto.
- El Instituto es responsable del suministro y uso de las herramientas referidas en el punto anterior y hará uso de las mismas para la ejecución del análisis de vulnerabilidades. El espíritu de ambos análisis es que el Proveedor ejecute un análisis de vulnerabilidades y en caso de requerirse aplique las soluciones necesarias; el Instituto con base en sus herramientas fortalecerá la investigación siempre en beneficio de tener un equipo libre de vulnerabilidades de seguridad.
- Configurar la solución de correo para que el envío de correos sea por autenticación.
- Configurar la solución de correo ofertada para que se integren con el administrador de cuentas de dominio del Instituto y/o formar parte de éste. La administración del dominio es responsabilidad del Instituto; ésta y el Proveedor definirán y delimitarán las respectivas responsabilidades del servicio de correo electrónico.
- Mantener al día la actualización de parches de seguridad que generen los fabricantes que aplique para el sistema operativo, servidores y para las soluciones de software que el Proveedor haya ofertado e implementado.
- Cuando el Instituto decida dar por terminado el servicio de administración de correo electrónico, el proveedor deberá emitir un certificado de borrado seguro de toda la información relacionada a este servicio

Confidencialidad

- El Proveedor deberá garantizar la confidencialidad de la información vinculada al resguardo y almacenamiento de las cuentas de correo electrónico.

3.2.7.1.2. Lync

Se requiere el servicio de mensajería instantánea con los siguientes requisitos mínimos:

Configuración del Servicio

- Contar con equipos de tecnología reciente y que los elementos de hardware que proponga deberán contar al menos con características redundantes como lo pueden ser:
  - Fuentes de poder
  - Procesadores
  - Discos duros
- Configurar la solución de Mensajería Instantánea Institucional en un esquema que permita tener los siguientes beneficios:
  - Presencia
  - Mensajería instantánea
  - Peer to peer para audio y video
  - Compartir escritorio
  - Transferencia de archivos
  - Conferencia
  - Mensajería en dispositivos móviles (Smartphone, tablet's)
- El escenario requerido por el IMSS para el servicio de Mensajería Instantánea Institucional es el siguiente:
  - Contemplar un ambiente para soportar 40,000 usuarios como mínimo, de los cuales:
    - 36,000 usuarios existentes en el instituto sobre plataforma actual se migraran a la plataforma ofertada por el proveedor.
    - Se deberá de contemplar en el ambiente nuevo, capacidad de cómputo para soportar 10,000 usuarios más.
    - Manejo de 2 Perfiles de usuarios "esto es enunciativo más no limitativo"; Básico y VIP
      - 32,000 cuentas de usuario (Básicos) con:
        - Mensajería Instantánea
        - Presencia
        - Conversación grupal
      - 4,000 cuentas de usuario (VIP) con:
        - Mensajería Instantánea
        - Presencia
        - Conversación Grupal
        - Conferencias Audio/Video 1:1
        - Conferencias Audio/Video grupal
        - Contenido Presentable
    - Compartir Escritorio

- Compartir Power Point
- Compartir Programa
- Compartir Archivos (Se debe limitar las extensiones de archivo)

- Contemplar esquema de alta disponibilidad en todos los roles
- Establecer un esquema de optimización que considere de manera enunciativa más no limitativa tareas como: desfragmentación de la base de datos del Servicio de Mensajería Instantánea Institucional, revisiones de integridad de la base de datos; depuración de logs del sistema operativo, servidores y de las soluciones diversas de antivirus, etc.
- Configurar las políticas de usuarios y políticas de Conferencias, se hará basado en hasta 3 perfiles, desde aquellos con solo audio, hasta aquellos con Video con calidad, CIF, VGA o HD

Las políticas se configuran a nivel servidor y se aplican a los usuarios o grupos de usuarios usando las herramientas de configuración correspondientes

Filtrado de contenido

El Proveedor deberá mantener el saneamiento del servicio de Mensajería Instantánea Institucional, por lo que la solución propuesta debe contar con software de antivirus licenciado tanto a nivel sistema operativo como a nivel aplicativo; el licenciamiento de este software deberá ser suministrado por el Proveedor. Así mismo, el proveedor deberá:

- Configurar herramientas de antivirus para que se realicen escaneos diarios del sistema operativo.
- Programar una tarea para que las definiciones de datos de la solución del antivirus se actualicen diariamente.
- Administrar de la solución de antivirus y tenerlo configurado con las mejores prácticas de administración que de manera enunciativa más no limitativa pueden ser: revisión en tiempo real, revisión de sector de arranque y memoria, análisis heurístico, limpieza automática, zonas de cuarentena, escaneo de scripts, etc.

La solución propuesta debe contar con software para protección de males de la Web como, esta solución debe ser tanto a nivel sistema operativo como a nivel aplicativo, por lo que el proveedor deberá:

- Contar con herramientas, para cumplir con el requerimiento anterior; la solución puede ser de hardware o de software según lo decida el Proveedor.
- Gestionar la administración de la herramienta de acuerdo a las mejores prácticas de administración que de manera enunciativa más no limitativa pueden ser:
  - Actualizar diariamente las bases de datos.
  - Bloquear de videos, música y/o imágenes.
  - Bloquear lenguaje pornográfico y/o alto contenido sexual.

Lo anterior previa validación y autorización del Instituto.

Las actualizaciones de la protección de malware e incluso el antivirus deben realizarse diariamente.

Respaldos y Restauración de la Información

El Proveedor deberá establecer un esquema de respaldos en línea y restauración de las bases de datos con los siguientes requerimientos:

- Considerar el respaldo total de la base.
- El respaldo debe hacerse con periodicidad diaria, semanal y mensual.
- Realizarse en medios magnéticos u otro medio que sea externo al servidor.
- Conservar los respaldos semanales y mensuales en una bóveda externa, de modo que los únicos respaldos que podrán permanecer en el centro de datos primario serán los diarios.

El Proveedor debe proporcionar el licenciamiento necesario en el software de respaldos para lograr el respaldo en línea

Seguridad y Vulnerabilidad

El Proveedor deberá establecer un esquema de seguridad que proteja los bienes involucrados en la solución del servicio de Mensajería Instantánea Institucional, por lo que debe considerar al menos lo siguiente:

- Establecer un procedimiento de análisis de vulnerabilidades con base en herramientas comerciales que permita identificar si la solución ofertada está libre de vulnerabilidades conocidas; se deberá entregar un reporte al menos trimestral de dicho análisis.
- Tener la solución ofertada 100% libre de vulnerabilidades conocidas. En caso de que el servicio ofertado sea objeto de un ataque exitoso se aplicarán las deducciones correspondientes.
- Suministrar y utilizar sus propias herramientas de análisis de vulnerabilidades para cumplir con lo solicitado en el presente Anexo Técnico. Éstas no necesariamente deben de ser las mismas con las que cuenta el Instituto.
- El Instituto puede en cualquier momento ejecutar con sus propias herramientas para el análisis de vulnerabilidades (Con las que cuente el área de seguridad informática del Instituto en ese momento), en caso de detección de éstas, el Proveedor estará obligado a solucionarlas en un plazo no mayor a 3 días. No necesariamente por cada análisis del Proveedor habrá un análisis del Instituto.
- El Instituto es responsable del suministro y uso de las herramientas referidas en el punto anterior y hará uso de las mismas para la ejecución del análisis de vulnerabilidades. El espíritu de ambos análisis es que el Proveedor ejecute un análisis de vulnerabilidades y en caso de requerirse aplique las soluciones necesarias; el Instituto con base en sus

herramientas fortalecerá la investigación siempre en beneficio de tener un equipo libre de vulnerabilidades de seguridad.

- Configurar la solución de Mensajería Instantánea Institucional para que el acceso a las cuentas sea por autenticación.
- Configurar la solución de Mensajería Instantánea Institucional ofertada para que se integren con el administrador de cuentas de dominio del Instituto y/o formar parte de éste. La administración del dominio es responsabilidad del Instituto; ésta y el Proveedor definirán y delimitarán las respectivas responsabilidades del servicio de Mensajería Instantánea Institucional.
- Mantener al día la actualización de parches de seguridad que generen los fabricantes que aplique para el sistema operativo, servidores y para las soluciones de software que el Proveedor haya ofertado e implementado.

Confidencialidad

El Proveedor deberá garantizar la confidencialidad de la información vinculada al resguardo y almacenamiento de las cuentas de Mensajería Instantánea Institucional.

4. Operación Digital

4.1. Servicios Generales

4.1.1. Dirección ejecutiva y gestión

Gestión del portafolio (cartera)

4.1.1.1.1. Gestor del Portafolio de proyectos (PPM)

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma Project Portfolio Management o equivalente según sus necesidades. El licitante deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de Project Portfolio Management o equivalente (soporte empresarial)
- Version del producto 9.22 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

4.1.2. Gestión de la seguridad cibernética

Identificación y autenticación

4.1.2.1.1. Usuario de Acceso a la Nube Privada

Creación del usuario en la plataforma

Asignación de roles, permisos y acceso a recursos

Asociación de perfil con hasta 5 dispositivos

Tarjeta inteligente asociada a la identidad que cumpla con las siguientes características:

- Debe aceptar formatos ID-1
- Cumplir con el estándar ISO 7816
- Utilizar algoritmos criptográficos como RSA, DES, 3DES, AES, and SHA
- Todo software necesario en el cliente para su correcta instalación y operación, compatibles con las versiones de Windows soportadas por Microsoft

Licenciamiento de gestión de identidad y control de acceso

Gestión de la seguridad

4.1.2.1.2. Servicio de Seguridad Perimetral para Enlaces de Banda Ancha.

El instituto requiere un servicio que permita proporcionar la infraestructura que brinde seguridad perimetral para enlaces de banda ancha, a través de los cuales se establece la transferencia de información entre diferentes unidades médicas y administrativas del IMSS.

El servicio de seguridad perimetral para enlaces de banda ancha se requiere en dos modalidades:

- Sitios con un ancho de banda mayor a 100 Mbps y hasta 1 Gbps
- Sitios con un ancho de banda de hasta 100 Mbps.

Las características principales que debe reunir el servicio para Sitios con un ancho de banda mayor a 100 Mbps y hasta 1 Gbps:

- Deberá contar al menos con un rendimiento de 8 Gbps, en su funcionalidad de firewall.
- Deberá tener al menos un rendimiento 1.2 Gbps en su funcionalidad de IPS

- Mínimo deberá contar con 12 puertos 100/1000 de cobre RJ45
- Mínimo deberá contar con 4 puertos de 1 Gbps de fibra
- Mínimo deberá contar con 2 puertos de 10 Gbps de fibra
- Deberá ser un dispositivo de nivel empresarial
- Deberá ser un dispositivo multifuncional, es decir integrar las funcionalidades descritas a continuación, en un solo dispositivo dedicado:
  - Firewall
  - Detección y prevención de intrusos (IPS)
  - Filtrado de contenido de la WEB
  - Detección y control de virus
  - Detección y control de amenazas y programas maliciosos
  - Protección para correo electrónico
  - Detección y control de correo no deseado
- Deberá contar con una consola de administración integrada accesible vía remota y a través de interfaz RJ45
- Deberá contar con doble fuente de poder que pueda ser sustituida en caliente sin afectar al dispositivo y al servicio que presta
- Deberá garantizar técnicamente la seguridad de datos, en situaciones como accesos remotos y comunicaciones de sitio a sitio
- Deberá ser compatible con direccionamiento IPv4 e IPv6
- Deberá contar con la capacidad de manejo de al menos 1024 Vlans.
- Deberá poder operar de manera transparente como un dispositivo Capa 2 y como un dispositivo de ruteo en Capa 3.
- Deberá operar en alta disponibilidad tomando en cuenta los siguientes esquemas:
  - Modo ruteo en capa 3 Activo-Activo
  - Modo ruteo en capa 3 Activo-Pasivo
  - Modo balanceo de carga y conmutación por error.
  - Modo VRRP
- Deberá incluir la capacidad de generar al menos 15,000 túneles VPN a través del protocolo IPSec.
- Deberá poder aplicar QoS (Quality of Service) para priorizar tráfico de Datos, Voz y Video
- Deberá poder crear políticas granulares es decir:
  - Para usuarios
  - Para grupos

Además deberá identificar, permitir, bloquear o limitar el uso de aplicaciones independientemente del puerto, protocolo o técnica evasiva.

- Deberá permitir el escaneo de aplicaciones tales como mensajería instantánea, redes sociales, streaming de video, Voz sobre IP, juegos entre otras.
- Deberá poder realizar autenticación de usuarios a través de Directorio Activo (LDAP), Portal Cautivo, Kerberos, Radius, Tacacs.

- Deberá contar con la administración centralizada de acceso a usuarios, a los recursos del Instituto y aplicaciones en Internet
- Deberá permitir la conexión a las aplicaciones del Instituto a través de dispositivos móviles (Tablet's, SmartPhone's)

Las características principales que debe reunir el servicio para Sitios con un ancho de banda de hasta 100 Mbps:

- Deberá contar al menos con un rendimiento de 3 Gbps, en su funcionalidad de firewall.
- Deberá tener al menos un rendimiento 600 Mbps en su funcionalidad de IPS
- Mínimo deberá contar con 8 puertos 100/1000 de cobre RJ45
- Mínimo deberá contar con 4 puertos de 1 Gbps de fibra
- Deberá ser un dispositivo de nivel empresarial
- Deberá ser un dispositivo multifuncional, es decir integrar las funcionalidades descritas a continuación, en un solo dispositivo dedicado:
  - Firewall
  - Detección y prevención de intrusos (IPS)
  - Filtrado de contenido de la WEB
  - Detección y control de virus
  - Detección y control de amenazas y programas maliciosos
  - Protección para correo electrónico
  - Detección y control de correo no deseado
- Deberá contar con una consola de administración integrada accesible vía remota y a través de interfaz RJ45
- Deberá garantizar técnicamente la seguridad de datos, en situaciones como accesos remotos y comunicaciones de sitio a sitio
- Deberá ser compatible con direccionamiento IPv4 e IPv6
- Deberá contar con la capacidad de manejo de al menos 512 Vlans.
- Deberá poder operar de manera transparente como un dispositivo Capa 2 y como un dispositivo de ruteo en Capa 3.
- Deberá operar en alta disponibilidad tomando en cuenta los siguientes esquemas:
  - Modo ruteo en capa 3 Activo-Activo
  - Modo ruteo en capa 3 Activo-Pasivo
  - Modo balanceo de carga y conmutación por error.
  - Modo VRRP
- Deberá incluir la capacidad de generar al menos 10,000 túneles VPN a través del protocolo IPSec.
- Deberá poder aplicar QoS (Quality of Service) para priorizar tráfico de Datos, Voz y Video
- Deberá poder crear políticas granulares es decir:
  - Para usuarios
  - Para grupos
- Además deberá identificar, permitir, bloquear o limitar el uso de aplicaciones independientemente del puerto, protocolo o técnica evasiva.

- Deberá permitir el escaneo de aplicaciones tales como mensajería instantánea, redes sociales, streaming de video, Voz sobre IP, juegos entre otras.
- Deberá poder realizar autenticación de usuarios a través de Directorio Activo (LDAP), Portal Cautivo, Kerberos, Radius, Tacacs.
- Deberá contar con la administración centralizada de acceso a usuarios, a los recursos del Instituto y aplicaciones en Internet
- Deberá permitir la conexión a las aplicaciones del Instituto a través de dispositivos móviles (Tablet's, SmartPhone's)

4.1.3. Intercambio de Información

Herramientas de colaboración

4.1.3.1.1. SharePoint

Se requiere el servicio de la administración de la plataforma de Colaboración Institucional basada en Microsoft SharePoint o equivalente, durante la vigencia del contrato.

Los requisitos mínimos que el proveedor deberá considerar son:

Configuración del Servicio

- Contar con equipos de tecnología reciente y que los elementos de hardware que proponga deberán contar al menos con características redundantes como lo pueden ser: Fuentes de poder, Procesadores y Discos duros.
- La configuración de la solución deberá ser una granja "grande" de servidores.
- La configuración deberá contemplar un tamaño en número de usuarios de 22,000 como mínimo y un número de documentos de 440,000, como mínimo.
- Se requiere como mínimo una implementación de tres niveles en la granja: los servidores front-end y web en el primer nivel, los servidores de aplicaciones en el segundo nivel, y el servidor de bases de datos en el tercer nivel.
- Los requisitos mínimos de hardware para los servidores web, front-end y de aplicación deberán ser:
  - RAM: 12 GB, PROCESADOR: 64 bits, 4 núcleos, DISCO DURO: 80 GB para la unidad de sistema
- Los requisitos mínimos de hardware, para el servidor de Base de Datos deberá ser:
  - PROCESADOR: 64 bits, 8 núcleos, RAM: 16 GB, DISCO DURO: 80 GB para la unidad de sistema.
- Los requisitos mínimos de Software para los servidores web, front-end y servidores de aplicación deberán ser:
  - Microsoft SharePoint 2013
  - Edición de 64 bits de Windows Server 2012 Standard o Datacenter

- El proveedor deberá instalar los siguientes requisitos para los servidores web, front-end y de aplicación:
  - Rol Servidor web (IIS)
  - Rol Servidor de aplicaciones
  - Microsoft .NET Framework, versión 4.5
  - Servicios de datos WCF 5.0 de Microsoft
  - Microsoft Information Protection and Control Client (MSIPC)
  - Microsoft Sync Framework Runtime v1.0 SP1 (x64)
  - Windows Management Framework 3.0, que incluye Windows PowerShell 3.0
  - Windows Server AppFabric
- Los requisitos mínimos para el servidor de base de datos deberá considerar:
  - La edición de 64 bits de Microsoft SQL Server 2012.
  - La edición de 64 bits de Windows Server 2012 Standard o Datacenter.
  - Configuraciones de IIS 7.5 no se actualizan al usar la clase ServerManager para confirmar los cambios de configuración (KB 2708075).
  - Configuración de ASP.NET (SharePoint) en .NET 4.5 RTM.
  - Windows Server 2012 (KB 2765317)
  - Microsoft .NET Framework, versión 4.5

Filtrado de contenido

El Proveedor deberá mantener el saneamiento del servicio de la plataforma de Colaboración Institucional basada en Microsoft SharePoint, por lo que la solución propuesta debe contar con software de antivirus licenciado tanto a nivel sistema operativo como a nivel aplicativo; el licenciamiento de este software deberá ser suministrado por el Proveedor. Así mismo, el proveedor deberá:

- Configurar herramientas de antivirus para que se realicen escaneos diarios del sistema operativo.
- Programar una tarea para que las definiciones de datos de la solución del antivirus se actualicen diariamente.
- Administrar de la solución de antivirus y tenerlo configurado con las mejores prácticas de administración que de manera enunciativa más no limitativa pueden ser: revisión en tiempo real, revisión de sector de arranque y memoria, revisión de archivos comprimidos, análisis heurístico, limpieza automática, zonas de cuarentena, escaneo de scripts, etc.

Respaldos y Restauración de la Información

El Proveedor deberá establecer un esquema de respaldos en línea y restauración de las bases de datos de contenido y las de servicio, con los siguientes requerimientos:

- Considerar el respaldo total de las bases de datos.
- El respaldo debe hacerse con periodicidad diaria, semanal y mensual.
- Los respaldos diarios tendrán un reciclaje de 7 días, los semanales de 4 semanas y los mensuales de 1 año.

- Realizarse en medios magnéticos u otro medio que sea externo al servidor.
- Conservar los respaldos semanales y mensuales en una bóveda externa, de modo que los únicos respaldos que podrán permanecer en el centro de datos primario serán los diarios.
- El Proveedor debe proporcionar el licenciamiento necesario en el software de respaldos para lograr el respaldo en línea

Seguridad y Vulnerabilidad

El Proveedor deberá establecer un esquema de seguridad que proteja los bienes involucrados en la solución del servicio de la plataforma de Colaboración Institucional basada en Microsoft SharePoint, por lo que debe considerar al menos lo siguiente:

- Establecer un procedimiento de análisis de vulnerabilidades con base en herramientas comerciales que permita identificar si la solución ofertada está libre de vulnerabilidades conocidas; se deberá entregar un reporte al menos trimestral de dicho análisis.
- Tener la solución ofertada 100% libre de vulnerabilidades conocidas. En caso de que el servicio ofertado sea objeto de un ataque exitoso se aplicarán las deducciones correspondientes.
- Suministrar y utilizar sus propias herramientas de análisis de vulnerabilidades para cumplir con lo solicitado en el presente Anexo Técnico. Éstas no necesariamente deben de ser las mismas con las que cuenta el Instituto.
- El Instituto puede en cualquier momento ejecutar con sus propias herramientas para el análisis de vulnerabilidades (Con las que cuente el área de seguridad informática del Instituto en ese momento), en caso de detección de éstas, el Proveedor estará obligado a solucionarlas en un plazo no mayor a 3 días. No necesariamente por cada análisis del Proveedor habrá un análisis del Instituto.
- El Instituto es responsable del suministro y uso de las herramientas referidas en el punto anterior y hará uso de las mismas para la ejecución del análisis de vulnerabilidades. El espíritu de ambos análisis es que el Proveedor ejecute un análisis de vulnerabilidades y en caso de requerirse aplique las soluciones necesarias; el Instituto con base en sus herramientas fortalecerá la investigación siempre en beneficio de tener un equipo libre de vulnerabilidades de seguridad.
- Mantener al día la actualización de parches de seguridad que generen los fabricantes que aplique para el sistema operativo, servidores y para las soluciones de software que el Proveedor haya ofertado e implementado.
- Cuando el Instituto decida dar por terminado el servicio de administración de la plataforma de Colaboración Institucional basada en Microsoft SharePoint, el proveedor deberá emitir un certificado de borrado seguro de toda la información relacionada a este servicio.

Confidencialidad

- El Proveedor deberá garantizar la confidencialidad de la información vinculada al resguardo y almacenamiento de la plataforma de Colaboración Institucional basada en Microsoft SharePoint

4.1.4. Soporte para la entrega de servicios institucionales

Infraestructura Web

4.1.4.1.1. Servicio de Web

Considera toda la infraestructura que incluya el servicio de hosting de página web que oferte el Proveedor, el software que se requiera para cumplir lo solicitado por el Instituto en el presente Anexo Técnico, así como los servicios de administración, los servicios de respaldos, etc. El Instituto suministrará todo el licenciamiento de productos Microsoft necesarios para el servicio.

El Instituto requiere el servicio de hospedaje de página Web durante la vigencia del contrato con al menos las siguientes características:

- Se requiere un esquema de servicio continuo de 7x24x365, para lo cual el proveedor deberá de proveer del hardware y software necesario para lograr el nivel solicitado.
- El Instituto considera que para lograr el nivel de disponibilidad solicitado, la oferta del proveedor deberá considerar que los equipos sean nuevos y de tecnología reciente y que los elementos de hardware que proponga deberán contar al menos con características redundantes como lo pueden ser: Fuentes de poder, procesadores, Bios, y/o Discos duros. Por tecnología reciente se entiende, de manera enunciativa más no limitativa, equipos con al menos 2 procesadores Quad Xeón, discos duros SAS o SCSI de 15000 RPM, arreglos de disco RAID 1 para sistema operativo y RAID 5 para datos y bases de datos, memoria RAM de al menos 800 MHz.
- La solución de hardware propuesta deberá ser de arquitectura Intel para soportar sistemas operativos Microsoft Windows 2008 Server; con base en lo anterior se solicita que la plataforma propuesta sea compatible 100% con dicho sistema operativo.
- El Proveedor deberá instalar en la plataforma propuesta el sistema operativo Windows 2008 Server en ambiente de directorio activo, este software será proporcionado por el Instituto.
- El Proveedor deberá descargar de la Web, instalar y configurar de acuerdo a como lo indique el Instituto las aplicaciones de: Tomcat, PHP, PHP MyAdmin, MySQL y Joomla.
- El Proveedor deberá instalar el software MS SQL Server en su versión 2000, 2005 o 2008; el Instituto le enviará al Proveedor las instrucciones para la generación de las bases de

datos correspondientes y le enviará un respaldo de las mismas para que las restaure dentro de la solución ofertada; éste software será proporcionado por el Instituto.

- La solución propuesta deberá contar con software de antivirus a nivel sistema operativo, el cual deberá ser proporcionado por el Proveedor.
- El Proveedor deberá configurar dicha herramienta para que se realicen escaneos diarios del sistema.
- El Proveedor deberá programar una tarea para que las definiciones de datos de la solución del antivirus se actualicen diariamente.
- La administración de la solución antivirus será responsabilidad del Proveedor, éste se compromete a tenerlo configurado con las mejores prácticas de administración que de manera enunciativa más no limitativa pueden ser: revisión en tiempo real, revisión de sector de arranque y memoria, revisión de archivos comprimidos, análisis heurístico, limpieza automática, zonas de cuarentena, escaneo de scripts, etc.
- El Instituto podrá solicitar configuraciones personalizadas de las soluciones.
- El Proveedor deberá establecer un esquema de seguridad que proteja los bienes involucrados en la solución de servicio de hospedaje de página Web propuesta.
- El Proveedor deberá establecer un procedimiento de análisis de vulnerabilidades con base en herramientas comerciales que permita identificar si la solución ofertada está libre de vulnerabilidades conocidas; se deberá entregar un reporte al menos trimestral de dicho análisis.
- El Proveedor está obligado en tener la solución ofertada 100% libre de vulnerabilidades conocidas. En caso de que el servicio ofertado sea objeto de un ataque exitoso se aplicarán las deducciones correspondientes.
- El Instituto podrá en cualquier momento ejecutar sus propias herramientas para el análisis de vulnerabilidades (eEye Retina, AppDetective y Core Impact, además del software Microsoft Base Security analyzer), en caso de detección de éstas el Proveedor estará obligado a solucionarlas en un plazo no mayor a 3 días. No necesariamente por cada análisis del Proveedor habrá un análisis del Instituto.
- El Instituto será responsable del suministro y uso de las herramientas referidas en el punto anterior y hará uso de las mismas para la ejecución del análisis de vulnerabilidades. El espíritu de ambos análisis es que el Proveedor ejecute un análisis de vulnerabilidades y en caso de requerirse aplique las soluciones necesarias; el Instituto con base en sus herramientas fortalecerá la investigación siempre en beneficio de tener un equipo libre de vulnerabilidades de seguridad.
- El Proveedor deberá suministrar y utilizar sus propias herramientas de análisis de vulnerabilidades para cumplir con lo solicitado en las presentes bases. Éstas no necesariamente deben de ser las mismas con las que cuenta el Instituto.
- El Proveedor deberá instalar, configurar y mantener durante la vigencia del contrato el servicio de DNS externo de acuerdo a las configuraciones que el Instituto le provea.
- El Proveedor deberá instalar y configurar inicialmente el servicio de Internet Information Server y habilitar los accesos por puerto 80 y 443 según le defina el Instituto. A solicitud del Instituto se deberán poder dar de alta nuevos puertos para nuevas aplicaciones o servicios.

- El Proveedor proveerá inicialmente de 30 GB de espacio en disco duro para el almacenamiento de la página Web y de las bases de datos, se proyecta un crecimiento anual del 10%.
- El Proveedor deberá establecer un esquema de respaldos y restauración de las bases de datos y de carpetas del servidor (se incluye la página Web).
- El respaldo deberá considerar el respaldo en línea ("En caliente") del total de las bases de datos.
- El respaldo deberá considerar el respaldo total de todos los directorios que el Instituto defina.
- El respaldo deberá hacerse con periodicidad diaria, semanal y mensual.
- Los respaldos diarios tendrán un reciclaje de 7 días, los semanales de 4 semanas y los mensuales de 1 año.
- Los respaldos deberán realizarse en medios magnéticos u otro medio que sea externo al servidor.
- Los respaldos en medios magnéticos que deberán conservarse en la bóveda externa, deberán ser los semanales y mensuales. De modo que los únicos medios magnéticos que podrán permanecer en la cintoteca del centro de datos primario serán los diarios.
- La restauración deberá poder hacerse en forma completa e incluso por elemento, por ejemplo se deberá poder recuperar un solo archivo de una carpeta o se deberá poder recuperar una sola tabla de una base de datos.
- La restauración no deberá encimar o sobrescribir información que en esos momentos esté en línea, por consiguiente deberá permitir al personal del Instituto copiar de forma personalizada la información recuperada.
- El Instituto diariamente hace actualizaciones al sitio Web por lo que el Proveedor deberá implementar un esquema de publicación Web a través del enlace LAN to LAN solicitado en el presente Anexo Técnico.
- Inicialmente el Proveedor deberá instalar el certificado de seguridad con el que cuenta el Instituto, una vez que la vigencia del certificado venza el Proveedor deberá implementar y configurar dentro del servidor el certificado que le proporcione el Instituto, el cual deberá ser SSL a 256 bits y deberá estar ligado al nombre DNS del Web. Estas características se deben de conservar durante la vigencia del contrato.
- El acceso al servicio de Web ofertado para los usuarios ubicados en las instalaciones del Instituto deberá ser a través del enlace LAN to LAN que se oferta en este mismo Anexo Técnico.
- El acceso al servicio de Web ofertado para los usuarios ubicados fuera de las instalaciones del Instituto, es decir toda aquella persona que consulta la página Web del Instituto, deberá ser a través de un enlace tipo E1. Este enlace será el mismo que se oferta para el servicio de correo. El enlace tipo E1 se deberá cotizar de forma mensual, con la posibilidad de incrementar o disminuir su ancho de banda a solicitud del Instituto de acuerdo a sus necesidades de operación, el precio mensual del servicio del enlace tipo E1 debe ser indicado en el Anexo G "Tabla de precios de los servicios".

ANEXOS
DIVISIÓN DE CONTRATOS

- El Proveedor será responsable de mantener al día la actualización de parches de seguridad que genere Microsoft y los fabricantes que apliquen para el sistema operativo, para el SQL Server y para todas aquellas utilerías referidas en esta sección del presente Anexo Técnico.
- El Proveedor deberá configurar el servicio del Internet Information Server de manera que todos los eventos sean registrados en los archivos de logs, éstos deberán ser copiados a uno de los servidores en el Centro de Datos Primario en horarios después de las 00:00 horas a un equipo que designará el Instituto; lo anterior con la finalidad de que el Instituto genere reportes con la herramienta Webtrends.
- El Proveedor deberá considerar que la solución de web ofertada deberá configurarse para que se integren con el dominio activo del Instituto (active directory) y/o formar parte de éste. Para lo anterior, el Proveedor deberá implementar en el Centro de Datos Primario, previo a la instalación del servicio de Web un servidor de active directory. Este servidor será el mismo utilizado para el servicio de correo electrónico.
- Las conexiones configuradas de active directory deberán hacerse a través del enlace LAN to LAN que se oferta en estas mismas bases.
- El Proveedor deberá considerar una etapa de migración del Web actual del Instituto hacia la solución ofertada, por lo que deberá realizar todas las actividades necesarias para que la migración se haga sin afectación del servicio para los usuarios; de manera enunciativa más no limitativa el Proveedor deberá considerar: creación de bases de datos, restauración de información, alta de la página Web, fortalecimiento de permisos, pruebas de acceso, etc.
- El Proveedor deberá asignar en sitio al menos un técnico que apoye al personal de soporte técnico del Instituto en las tareas de migración del servicio de Web.
- El Proveedor deberá realizar cualquier configuración que solicite el Instituto siempre y cuando ésta sea relacionada con la solución ofertada, más allá de las configuraciones personalizadas que ya fueron detalladas en esta sección.
- La administración del nombre de dominio ante NIC México es responsabilidad del Instituto, en caso de que hubiese algún cambio en cuanto a direccionamiento IP o alta de nuevos u otros dominios a configurar en el servicio de correo o de web, el Proveedor deberá reflejar los mismos en las soluciones que se ofertan en el presente Anexo Técnico.
- Existe un DNS secundario que es proporcionado por el proveedor del servicio de Internet, el Instituto proveerá al Proveedor la IP de este DNS secundario para que se hagan las configuraciones necesarias para transferencias de zonas.
- Será responsabilidad del Proveedor monitorear que se hagan las transferencias de zonas entre el DNS Primario y el DNS Secundario.
- El Proveedor deberá actualizar, en caso de que aplique por solicitud del Instituto, las nuevas versiones que libere Microsoft respecto al sistema operativo y el Microsoft SQL Server; lo anterior previo a un estudio de actualización, pruebas de software y validación de servicios. El Proveedor deberá participar de forma activa en dichas pruebas y validaciones, asignando personal con conocimientos técnicos adecuados.

- El Proveedor deberá asegurarse que todas las demás herramientas consideradas en esta sección se encuentren vigentes y actualizadas durante la vigencia del contrato, el Instituto podrá solicitar en cualquier momento evidencia de este punto.

4.1.4.1.2. Software Multiplataforma de Administración de Activos

El Software Multiplataforma de Administración de Activos debe permitir al Instituto:

- Tener una solución de inventario multiplataforma para detectar todos los dispositivos, descubrir instalaciones de software y medir su uso.
- Administrar toda la gama de modelos de licencias comerciales con que cuente el Instituto.
- Optimizar licencias, y contar con visibilidad del uso del software licenciado para minimizar riesgos de cumplimiento frente a todos los fabricantes de software comercial del Instituto.
- Identificar el software que se está utilizando en toda la red y conciliarlo dinámicamente con los derechos de licencia del Instituto.
- Tener una solución integrada de Administración de Activos de Software (SAM) a escala empresarial que permita gestionar las licencias de software en todas las plataformas: pc's, centro de datos, móviles, virtualización y nube.
- Contener paneles de gestión tipo Dashboard para funciones específicas que se pueden adaptar a los distintos usuarios autorizados del Instituto, permitiendo una reducción de las cargas administrativas para los administradores del programa de Administración de Activos de Software.
- Contar con una visión unificada de todos los activos de software y hardware, derechos de licencias y métricas de uso de aplicaciones.
- Aportar una vista consolidada de todos los activos de la red y más allá, permitiendo a los administradores del sistema utilizar una sola interfaz para Administrar distintos distribuidores de software y diversos tipos de dispositivos y ubicaciones. Los datos de inventario deberán importarse desde más de una fuente de inventario para abarcar toda la variedad de plataformas y sistemas operativos (Windows, OSX, Linux, Unix).
- Identificar automáticamente todas las instalaciones de software no utilizadas, permitiendo así desinstalar y recuperar las licencias fácilmente. Para aumentar la disponibilidad de licencias para otros usuarios.
- Identificar y gestionar activos virtuales en la Red.

5. Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Ing. Héctor Javier Reyes Oropeza	Titular de la División de Administración, Procesamiento y Almacenamiento		12/11/2019
Lic. Carlos Francisco Ramirez Del Rivero	Titular de la División de Administración y Continuidad de la Operación		12/11/2019
Mtro. Hector Martinez Valenzuela	Titular de la División de Telecomunicaciones		12/11/2019
Mtro. Alejandro Paniagua Ramirez	Titular de la División de Administración de Riesgos Tecnológicos		12/11/2019

Revisó	Cargo	Firma	Fecha
Ing. Javier Cortés López	Titular de la Coordinación Técnica de Operación de Servicios Tecnológicos		12/11/2019
Ing. Carlos Calderon Zacarias	Titular de la Coordinación Técnica de Redes y Telecomunicaciones		12/11/2019

Aprobó	Cargo	Firma	Fecha
Ing. Eduardo Oropeza Ortíz	Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional		12/11/2019

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

Servicios de Continuidad de la Nube IMSS 2020

Apéndice #2. Ubicaciones Geográficas

Contenido

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	14/10/2019	Elaboración de documento	Ing. Héctor Javier Reyes Oropeza Lic. Carlos Francisco Ramírez del Rivero Ing. Román Alejandro Rea Martínez Ing. Héctor Martínez Valenzuela
0.2	28/10/2019	Actualización del documento	Ing. Javier Cortés López Ing. Carlos Calderón Zacarías
1.0	12/11/2019	Aprobación del documento	Ing. Eduardo Oropeza Ortiz

1. Objetivo del documento

El objetivo del presente Apéndice es establecer las ubicaciones, que de manera enunciativa mas no limitativa, se consideran como iniciales de referencia para las modalidades de despliegue del servicio administrado objeto de esta Licitación, para los casos específicos previstos en el Anexo Técnico, apéndice, términos y condiciones, anexos, oferta del licitante, y documentación contractual, sin menoscabo de que éstas únicamente se requerirán por evento.

2. Consideraciones geográficas de centro de datos primario

Éste deberá estar ubicado en territorio nacional.

3. Ubicaciones iniciales de extensión de nube privada

En estas ubicaciones, que se enuncian de manera enunciativa mas no limitativa, el proveedor deberá entregar, instalar, habilitar, configurar, así como dar soporte y mantenimiento preventivo y correctivo, a aquella infraestructura solicitada por el Instituto que permita la operación de aplicativos y sistemas locales tales como, los Sistemas Integrales de Medicina Familiar (SIMF), SAI Farmacia, entre otros, así como sistemas propios de cada Unidad Médica, los cuales interactúan con los sistemas de cómputo centralizados que operan en el Centro de Datos Administrado.

Se consideran 15 ubicaciones iniciales que se distribuyen alrededor del territorio nacional, cubriendo los complejos Hospitalarios más relevantes para las operaciones Hospitalarias del Instituto. Cada complejo Hospitalario comprende unidades médicas de diferentes clasificaciones y niveles de atención, siendo un total de 39 complejos inicialmente (10 HE, 3 HGR, 4 UMF, 3 HGZMF, 4 HGO, 1 UMFR, 1 HGZ, 2 HP, 3 BS, 1 HGP, 1 HTO, 1 HG, 1 HI, 1 HC, 1 HON, 1 HO, 1 HT).

- SONORA - CD. OBREGÓN (3)
  - HE 2 CMN Noroeste Obregón: Calle del Seguro No. S/N, Unidad habitacional Multifamiliares IMSS C.P. 85120 Ciudad Obregón, Municipio de Cajeme, Sonora.
  - HGR 1 Cd. Obregón: Calle Prolongación Vicente Guerrero No. S/N, Unidad habitacional Infonavit C.P. 85120 Ciudad Obregón, Municipio de Cajeme, Sonora.
  - UMF 1 Obregón. Calle Prolongación Guerrero No. S/N, Unidad habitacional Infonavit C.P. 85120 Ciudad Obregón, Municipio de Cajeme, Sonora.
- COAHUILA - TORREÓN (2)
  - HE 71 Torreón: Boulevard Revolución No. S/N, Colonia Torreón Jardín C.P. 27200 Torreón, Municipio de Torreón, Coahuila de Zaragoza
  - HGZMF 16 Torreón: Boulevard Revolución No. S/N, Colonia Torreón Jardín C.P. 27200 Torreón, Municipio de Torreón, Coahuila de Zaragoza.
- NUEVO LEÓN - MONTERREY NORTE (1)
  - HE 25 Monterrey: Eje Metropolitano 36 esq Eje Metropolitano 10/ Av. Gonzalitos y Av. Lincoln No. S/N, Colonia Valle de las Mitras C.P. 64300 Monterrey, Municipio de Monterrey, Nuevo León.

- NUEVO LEÓN - MONTERREY SUR (4)
  - HGO 23 Monterrey: Avenida Constitución esq Félix U Gómez No. S/N, Colonia Obrera C.P. 64010 Monterrey, Municipio de Monterrey, Nuevo León.
  - HGZMF 2 Monterrey: Avenida Constitución y Profesor G. Torres No. S/N, Colonia Obrera C.P. 64010 Monterrey, Municipio de Monterrey, Nuevo León.
  - HGZ 33 Félix U. Gómez: Avenida Félix Uresti Gómez y Av. Ezequiel E. Chávez No. S/N, Colonia Obrera C.P. 64010 Monterrey, Municipio de Monterrey, Nuevo León.
  - UMFR 1 Monterrey: Avenida Constitución No. S/N, Colonia Obrera C.P. 64010 Monterrey, Municipio de Monterrey, Nuevo León.

- JALISCO - OCCIDENTE CMNO (5)
  - HE CMN Occidente: Calle Belisario Domínguez entre Salvador Quevedo y Zubieta y Sierra Morena No. 1000, Fraccionamiento Independencia Oriente C.P. 44340 Guadalajara, Municipio de Guadalajara, Jalisco.
  - HGO CMN Occidente: Calle Belisario Domínguez entre Salvador Quevedo y Zubieta y Sierra Morena No. 771, Fraccionamiento Independencia Oriente C.P. 44340 Guadalajara, Municipio de Guadalajara, Jalisco.
  - HP CMN Occidente: Calle Belisario Domínguez No. 735, Fraccionamiento Independencia Oriente C.P. 44340 Guadalajara, Municipio de Guadalajara, Jalisco.
  - UMF 3: Calle Belisario Domínguez No. 815, Colonia Independencia Oriente C.P. 44340 Guadalajara, Municipio de Guadalajara, Jalisco.
  - BS CMNO Occidente Calle Belisario Domínguez entre Salvador Quevedo y Zubieta y Sierra Morena No. 1000, Fraccionamiento Independencia Oriente C.P. 44340 Guadalajara, Municipio de Guadalajara, Jalisco.

- JALISCO - OCCIDENTE HGZ 46 (1)
  - HGR 46: Guadalajara Avenida Lázaro Cárdenas No. 1060, Colonia 8 de Julio C.P. 44910 Guadalajara, Municipio de Guadalajara, Jalisco.

- GUANAJUATO - BAJÍO (3)
  - HE 1 CMN del Bajío: Boulevard Adolfo López Mateos y Paseo de los Insurgentes No. S/N, Colonia Los Paraísos C.P. 37328 León de Los Aldama, Municipio de León, Guanajuato.
  - HGP 48 CMN del Bajío: Avenida Paseo de los Insurgentes No. S/N, Colonia Los Paraísos C.P. 37328 León de Los Aldama, Municipio de León, Guanajuato.
  - UMF 51 León: Avenida Paseo de los Insurgentes Esq. Av. México No. S/N, Colonia Los Paraísos C.P. 37328 León de Los Aldama, Municipio de León, Guanajuato.

- ESTADO DE MÉXICO - LOMAS VERDES (1)
  - HTO Lomas Verdes: Avenida Lomas Verdes esq Blvd. Manuel Ávila Camacho No. 52, Colonia Santa Cruz Acatlán C.P. 53150 Naucalpan de Juárez, Municipio de Naucalpan de Juárez, Estado de México.

- DISTRITO FEDERAL NORTE - LA RAZA (5)
  - HE CMN La Raza: Calle Seris No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Distrito Federal.
  - HGO 3 CMN La Raza: Avenida Vallejo esq Antonio Valeriano No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Distrito Federal.

  - HI CMN La Raza: Circuito Interior Paseo de las Jacarandas No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Distrito Federal.
  - HG CMN La Raza: Circuito Interior Paseo de las Jacarandas No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Distrito Federal.
  - BS CMN La Raza: Calle Seris No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Distrito Federal.

- DISTRITO FEDERAL NORTE - MAGDALENA DE LAS SALINAS (2)
  - HO Magdalena de las Salinas: Colector 15 S/N casi Esq. Av. I.P.N. Col. Magdalena de las Salinas, C.P. 07760, Gustavo A. Madero, D.F.
  - HT Magdalena de las Salinas: Colector 15 S/N Esq. Av. I.P.N. Col. Magdalena de las Salinas C.P. 07760, Gustavo A. Madero, D.F.

- DISTRITO FEDERAL SUR - SXXI (5)
  - HE CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Distrito Federal.
  - HP CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Distrito Federal.
  - HC CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Distrito Federal.
  - HONCO CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Distrito Federal.
  - BS CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Distrito Federal.

- DISTRITO FEDERAL SUR - SAN ANGEL (2)
  - HGO 4 CMN Siglo XXI San Angel Eje Vial Eje 10 Sur Río Magdalena No. 289, Colonia Tizapán San Ángel C.P. 1090 Álvaro Obregón, Delegación Álvaro Obregón, Distrito Federal.
  - HGZMF 8 San Ángel: Avenida Río Magdalena No. 289, Colonia Tizapán San Ángel C.P. 1090 Álvaro Obregón, Delegación Álvaro Obregón, Distrito Federal.

- PUEBLA - PUEBLA (2)
  - HE CMN Puebla: Calle 2 norte entre 24 y 18 Oriente No. 2004, Colonia Centro C.P. 72000 Heroica Puebla de Zaragoza, Municipio de Puebla, Puebla.
  - UMF: Calle 9 Oriente No. 420, Colonia Centro C.P. 72000 Heroica Puebla de Zaragoza, Municipio de Puebla, Puebla.

- VERACRUZ - VERACRUZ (1)
  - HE 14 Veracruz: Avenida Cuauhtémoc No. S/N, Colonia Formando Hogar C.P. 91810 Veracruz, Municipio de Veracruz, Veracruz de Ignacio de la Llave.

- YUCATAN - MÉRIDA (2)
  - HE CMN Mérida: Calle 41 entre la 34 y la 30 No. 439, Colonia Industrial C.P. 97150 Mérida, Municipio de Mérida, Yucatán.
  - HGR 1 Mérida: Calle 34 x 41 No. 439, Colonia Industrial C.P. 97150 Mérida, Municipio de Mérida, Yucatán.

Tipos de Unidades Médicas:

ANEXOS

DIVISIÓN DE CONTRATOS

- UMF Unidad de Medicina Familiar
- UMRM Unidad Médica Rural de Esquema Modificado
- UAMF Unidad Auxiliar de Medicina Familiar

- UMAA Unidad Médica de Atención Ambulatoria
- UMFR Unidad de Medicina Física y Rehabilitación
- BCS Banco de Sangre
- CCSM Centro Comunitario de Salud Mental
- HGZ Hospital General de Zona
- HGS Hospital General de Sub-Zona
- HGR Hospital General Regional
- HE Hospital de Especialidades
- HGO Hospital de Gineco Obstetricia
- HP Hospital de Pediatría
- HGP Hospital de Gineco Pediatría
- HTO Hospital de Traumatología y Ortopedia
- HT Hospital de Traumatología
- HORT Hospital de Ortopedia
- HON Hospital de Oncología
- HCARD Hospital de Cardiología
- HPS Hospital de Psiquiatría
- HINF Hospital de Infectología

Tabla resumen:

Ubicación	Unidades médicas	Tamaño Nodo
CD. OBREGON	3 (HE, HGR, UMF)	Ch
TORREON	2 (HE, HGZMF)	Ch
MONTERREY NORTE	1 (HE)	Ch
MONTERREY SUR	4 (HGZMF, HGO, UMFR, HGZ)	G
OCCIDENTE CMNO	5 (HE, UMF, HGO, HP, BS)	G
OCCIDENTE HGR 46	1 (HGR)	Ch
BAJÍO	3 (HE, UMF, HGP)	Ch
LOMAS VERDES	1 (HTO)	Ch
LA RAZA	5 (HE, HGO, HG, HI, BS)	G
SXXI	5 (HE, HP, HC, HON, BS)	G
SAN ANGEL	2 (HGZMF, HGO)	Ch
MAGDALENA DE LAS SALINAS	2 (HO,HT)	G
PUEBLA	2 (HE, UMF)	G
VERACRUZ	1 (HE)	Ch
MÉRIDA	2 (HE, HGR)	Ch
Total Unidades Médicas	39 (10 HE, 3 HGR, 4 UMF, 3 HGZMF, 4 HGO, 1 UMFR, 1 HGZ, 2 HP, 3 BS, 1 HGP, 1 HTO, 1 HG, 1 HI, 1 HC, 1 HON, 1 HO, 1 HT)	15 (6G, 9Ch)

Los tamaños del nodo que se especifican en la tabla anterior es referencial y podrán cambiar a solicitud del Instituto.

4. Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Ing. Héctor Javier Reyes Oropeza	Titular de la División de Administración, Procesamiento y Almacenamiento		12/11/2019
Lic. Carlos Francisco Ramírez Del Rivero	Titular de la División de Administración y Continuidad de la Operación		12/11/2019
Mtro. Hector Martinez Valenzuela	Titular de la División de Telecomunicaciones		12/11/2019
Mtro. Alejandro Paniagua Ramirez	Titular de la División de Administración de Riesgos Tecnológicos		12/11/2019

Revisó	Cargo	Firma	Fecha
Ing. Javier Cortés López	Titular de la Coordinación Técnica de Operación de Servicios Tecnológicos		12/11/2019
Ing. Carlos Calderon Zacarias	Titular de la Coordinación Técnica de Redes y Telecomunicaciones		12/11/2019

Aprobó	Cargo	Firma	Fecha
Ing. Eduardo Oropeza Ortiz	Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional		12/11/2019

Servicios de Continuidad de la Nube IMSS 2020

Apéndice #3. Esfuerzos realizados para la migración de centro de datos actual

ANEXOS

DIVISIÓN DE CONTRATOS

Contenido

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	14/10/2019	Elaboración de documento	Ing. Héctor Javier Reyes Oropeza Lic. Carlos Francisco Ramírez del Rivero Ing. Román Alejandro Rea Martínez Ing. Héctor Martínez Valenzuela
0.2	28/10/2019	Actualización del documento	Ing. Javier Cortés López Ing. Carlos Calderón Zacarías
1.0	12/11/2019	Aprobación del documento	Ing. Eduardo Oropeza Ortiz

1. Objetivo del documento

El objetivo del presente Apéndice es dar a conocer a los licitantes los esfuerzos realizados en la migración de aquellos sistemas migrados de los Centros de Datos del Instituto al Centro de Datos tercerizado a fin de que cuente con elementos para el cálculo de la propuesta para la fase de migración del servicio administrado objeto de esta Licitación, para lo previsto en el Anexo Técnico, así como la clasificación que a juicio del Instituto, tienen aquellos sistemas o aplicativos que fueron Implementados inicialmente en centro de datos tercerizado.

La información que se muestra a continuación está clasificada en términos de esfuerzo en Días/Hombre.

Para el cálculo de los esfuerzos de migración se tomaron en cuenta lo siguientes elementos:

- Tipo de Aplicaciones Institucionales
- Complejidad de las Aplicaciones
- Recursos Humanos

2. Tipos de Aplicaciones Institucionales

El Instituto clasifica los Aplicativos en criticidad complejo, mediano y bajo, de los cuales se tomaron los más significativos que reúnen las características necesarias para poder tomar la estimación de esfuerzo como una estimación confiable.

Las aplicaciones seleccionadas son:

- IMSS Desde su Empresa (IDSE) - Criticidad Alta
- Expediente Clínico Electrónico (ECE) – Criticidad Media
- Sharepoint y Team Foundation Server (SP y TFS) – Criticidad Media
- Folios de Incapacidad (FEPAC) – Criticidad Baja

3. Complejidad de las Aplicaciones

Las aplicaciones seleccionadas también fueron clasificadas tomando criterios de complejidad en la migración tales como:

- Complejo: Aplicaciones que dentro de su proceso de migración se consideraron escenarios que no permitían que los datos se pusieran en riesgo operativo, empleando mecanismos de replicación activa. Del mismo modo contienen múltiples elementos a migrar dentro de sus capas tecnológicas.
- Mediano: Aplicaciones que dentro de su proceso de migración involucraron la migración de datos y que son consideradas aplicaciones críticas dentro del Instituto. En este tipo de aplicaciones no se utilizaron mecanismos de replicación de datos activos. Del mismo modo contienen múltiples elementos a migrar dentro de sus capas tecnológicas.
- Bajo: Aplicaciones con pocos elementos en sus capas tecnológicas, los datos a migrar son pocos y no son aplicaciones críticas para el Instituto.

4. Recursos Humanos

Para considerar los recursos utilizados dentro de la migración se tomaron en cuenta los siguientes perfiles:

- Personal IMSS: Los recursos del Instituto que formaron parte de los esfuerzos de migración
- Fuerza de Trabajo: Perfiles del contrato de fuerza de trabajo actual que participaron en los esfuerzos de migración.
- Proveedores: Recursos especializados que fueron utilizados según la tecnología utilizada para la migración, tales como Microsoft, Oracle, etc.

5. Calendarios de Migración

Para el cálculo de esfuerzo de los recursos, se utilizaron como insumo los calendarios de migración y las bitácoras de los recursos para las aplicaciones seleccionadas, con la finalidad de poder contabilizar el total de horas invertidas para cada proyecto.

6. Tabla de esfuerzo de migración

Aplicativo	Esfuerzo en Días/Hombre				
IDSE	Fuerza de Trabajo	Oracle	Microsoft	IMSS	Total
Jefe de Departamento				120	
Coordinador de Proyectos				120	
Especialista Middleware B - 3 Años de exp	124				
Especialista Middleware C - 1 Año de exp	124				
Administrador Base de Datos A - 5 Años de exp	124				
Integrador B - 3 Años de exp	81				
Arquitecto A - 5 Años de exp	81				
Configurador A - 5 Años de exp	81				
Advanced Support Engineer - Base de Datos		223			
Advanced Support Engineer - Middleware		147			1,226

ECE	Fuerza de Trabajo	Oracle	Microsoft	IMSS	Total
Jefe de Departamento				80	
Coordinador de Proyectos				80	
Administrador Base de Datos A - 5 Años de exp	84				
Administrador Base de Datos B - 3 Años de exp	84				
Integrador B - 3 Años de exp	84				
Arquitecto A - 5 Años de exp	84				
Configurador A - 5 Años de exp	84				
Advanced Support Engineer - Base de Datos		5			585

SHAREPOINT y TFS	Fuerza de Trabajo	Oracle	Microsoft	IMSS	Total
Jefe de Departamento				80	
Coordinador de Proyectos				80	
Gestor de Contenido A - 5 Años de exp	52				
Especialista en Administracion del ciclo de vida de aplicaciones B - 3 Años de exp	52				
Gestor de Contenido B - 3 Años de Exp	52				
Administrador de la plataforma microsoft Windows A - 5 Años de exp	52				
Administrador de Proyectos A - 5 Años de exp	52				
PAFE SharePoint (Microsoft)			50		
PAFE SQL (Microsoft)			25		

PAFE TFS (Microsoft)			50		
DSEs SharePoint (Microsoft)			34		
DSEs SQL (Microsoft)			11		590

FEPAC	Fuerza de Trabajo	Oracle	Microsoft	IMSS	Total
Jefe de Departamento				40	
Coordinador de Proyectos				40	
Integrador B - 3 Años de exp	68				
Analista B - 3 Años de exp	68				
Configurador A - 5 Años de exp	68				
Advanced Support Engineer - Base de Datos		12			296

En resumen los esfuerzos aproximados en Días/Hombre por tipo de aplicación se resumen en lo siguiente:

- Complejas 1,200 Días/Hombre
- Medianas 600 Días/Hombre
- Bajas 300 Días/Hombre

Es importante mencionar que el esfuerzo mencionado, puede variar con motive de la evolución que los sistemas o aplicaciones hayan podido tener en el Centro de Datos Tercerizado.

7. Aplicaciones Migradas

No	Sistema	Área Usuaria	Tipo Aplicativo	Tipo Aplicativo	Esfuerzo D/H
1	Acceder Unificado	DIR	Implementado inicialmente en centro de datos externo	Complejo	
2	Analítica de Comprobación de Supervivencia	DPES	Implementado inicialmente en centro de datos externo	Mediano	
3	Directorio Activo	TODAS	Migrado	Complejo	1200
4	Consulta de Acuerdos Públicos	SG	Migrado	Bajo	300

ANEXOS
DIRECCIÓN DE CONTRATOS

5	Administración de Usuarios de los Servicios Digitales	DIR	Implementado inicialmente en centro de datos externo	Mediano	
6	Almacenes de Datos de Operación	DIR	Implementado inicialmente en centro de datos externo	Bajo	
7	Alta patronal Persona Moral No presencial SAS	DIR	Implementado inicialmente en centro de datos externo	Mediano	
8	Alta patronal Persona Moral No presencial	DIR	Implementado inicialmente en centro de datos externo	Bajo	
9	Alta Patronal Persona Física con CURP	DIR	Implementado inicialmente en centro de datos externo	Bajo	
10	Alta Patronal Persona Física No presencial	DIR	Implementado inicialmente en centro de datos externo	Bajo	
11	Access Managment 6.0 IMSS Digital	TODAS	Implementado inicialmente en centro de datos externo	Complejo	
12	Aplicación Móvil IMSS Digital	TODAS	Implementado inicialmente en centro de datos externo	Mediano	
13	Administración para la Publicación de Documentos de Enajenaciones por Venta de Bienes Muebles	DA	Migrado	Bajo	300
14	Administración para la Publicación de Documentos Licitatorios	DA	Migrado	Bajo	300
15	Asignación y Localización de NSS (ASigNSS)	DIR	Implementado inicialmente en centro de datos externo	Complejo	
16	Auto Proveedor Autorizado de Certificación	DA	Migrado	Complejo	1200
17	Régimen de Incorporación de la Seguridad Social	DIR	Implementado inicialmente en centro de datos externo	Mediano	
18	BMC-Remedy	DIDT	Migrado	Complejo	1200

19	Corrección de Datos del Asegurado	DIR	Implementado inicialmente en centro de datos externo	Mediano	
20	Actualización Dato CURP	DIR	Implementado inicialmente en centro de datos externo	Bajo	
21	Correo Electrónico Institucional	TODAS	Migrado	Complejo	1200
22	Comprobante Fiscal Digital a través de Internet de pagos patronales	DIR	Implementado inicialmente en centro de datos externo	Mediano	
23	Componente Habilitador Bóveda Personal	TODAS	Implementado inicialmente en centro de datos externo	Complejo	
24	Componente Habilitador de Firma Electrónica Criptografía y Notaría	DIR	Migrado	Complejo	1200
25	Semáforo de Diabetes Mellitus y de Hipertensión Arterial para Derechohabientes del IMSS	DPM	Implementado inicialmente en centro de datos externo	Bajo	
26	Código Infarto	DPM	Implementado inicialmente en centro de datos externo	Mediano	
27	Comunidad IMSS Digital	TODAS	Implementado inicialmente en centro de datos externo	Mediano	
28	Control de Movimientos Afiliatorios de Auditoria a Patrones	DIR	Migrado	Bajo	300
29	Comunidades Virtuales	TODAS	Migrado	Mediano	600
30	Consulta de Adeudo por Motivo de Cobro - Consulta de Adeudo	DIR	Implementado inicialmente en centro de datos externo	Bajo	
31	Consulta del Dictamen	DIR	Implementado inicialmente en centro de datos externo	Bajo	
32	Generación de Carta de No Adeudo de acuerdo al Código Fiscal de la Federación	DIR	Implementado inicialmente en centro de datos externo	Bajo	
33	Cédula de Riesgo e Información Integral del Patrón	DIR	Implementado inicialmente en centro de datos	Bajo	

			externo		
34	Componte Seguridad para el Control de Acceso a Aplicaciones	DIR	Implementado inicialmente en centro de datos externo	Complejo	
35	Control de Servicios Integrales	DPM	Migrado	Mediano	600
36	Cubos de Información Cifras del Empleo	DIR	Migrado	Mediano	600
37	Centro Virtual de Operaciones en Emergencias y Desastres	DPM	Migrado	Bajo	300
38	Inscripción a la Continuación Voluntaria al Régimen Obligatorio	DIR	Implementado inicialmente en centro de datos externo	Bajo	
39	Declaración Anual Patronal vía SUA	DIR	Migrado	Bajo	300
40	Sistema de Planeación de Recursos Institucionales - Inversiones Financieras v9.1	DF	Migrado	Mediano	600
41	DataMart Afiliación (Repositorio de Información)	DIR	Migrado	Mediano	600
42	DataMart Cobranza (Repositorio de Información)	DIR	Migrado	Mediano	600
43	DataMart Información IMSS-SAT (Repositorio de Información)	DIR	Migrado	Mediano	600
44	DataMart Pensiones	DPES	Migrado	Mediano	600
45	DataMart de SIAIS (Repositorio de Información)	DPM	Migrado	Mediano	600
46	DataMart Subsidios y Ayudas	DPES	Migrado	Mediano	600
47	Directory Services IMSS Digital	DIR	Implementado inicialmente en centro de datos externo	Mediano	
48	Expediente Clínico Electrónico	DPM	Migrado	Mediano	600
49	Educación a Distancia (SIED)	DPM	Migrado	Bajo	300
50	E-Learning	TODAS	Migrado	Bajo	300
51	Emisor	TODAS	Migrado	Bajo	300
52	Escritorio Virtual	DIR	Implementado inicialmente en centro de datos externo	Complejo	
53	Factura Electrónica	DA	Migrado	Mediano	600

54	Folios Electrónicos para la Administración Central / Certificado de Incapacidad Manual	DPM	Migrado	Mediano	600
55	Folios Electrónicos para la Administración Central / Salud en el Trabajo	DPM	Migrado	Mediano	600
56	Sistema de Planeación de Recursos Institucionales Fondo de Investigación en Salud v9.1	DPM	Migrado	Mediano	600
57	Sistema de Gestión de Remates	DIR	Migrado	Bajo	300
58	IMSS Desde su Empresa	DIR	Migrado	Complejo	1200
59	Incapacidad por Internet	DPES	Implementado inicialmente en centro de datos externo	Bajo	
60	Intranet	TODAS	Migrado	Mediano	600
61	Incorporación al Seguro de Salud para la Familia	DIR	Implementado inicialmente en centro de datos externo	Bajo	
62	Incorporación Voluntaria al Régimen Obligatorio	DIR	Implementado inicialmente en centro de datos externo	Bajo	
63	Juicio Contencioso Administrativo Federal IMSS Actor, Amparos y Recursos	DJ	Migrado	Bajo	300
64	Gestión de Clasificación de Empresas MAC II IMSS DIGITAL	DIR	Implementado inicialmente en centro de datos externo	Mediano	
65	Diario de Maternidad	DPES	Implementado inicialmente en centro de datos externo	Bajo	
66	Movimientos Patronales	DIR	Implementado inicialmente en centro de datos externo	Mediano	
67	Nuevo Esquema de Comprobación de Supervivencia de Pensionados en el Extranjero	DPES	Implementado inicialmente en centro de datos externo	Bajo	
68	Notificaciones por Estrados Electrónicos	DIR	Implementado inicialmente en centro de datos externo	Mediano	

ANEXOS

DIRECCIÓN DE CONTRATOS

69	Nuevo Sistema Monitor de Incapacidades	DPM	Migrado	Bajo	300
70	Nuevo Sistema de Subsidios y Ayudas	DPES	Migrado	Mediano	600
71	Oracle Data Integrator IMSS Digital	TODAS	Implementado inicialmente en centro de datos externo	Complejo	
72	Plataforma Analítica de Inteligencia de Negocios SAS-Miner	DIR	Migrado	Mediano	600
73	Portal de Incumplimientos	DA	Migrado	Bajo	300
74	Sistema de Planeación y Control de Alimentos	DPM	Migrado	Bajo	300
75	Portal de Compras	DA	Migrado	Mediano	600
76	Portal de Datos Abiertos	TODAS	Migrado	Bajo	300
77	Portal de Proveedores	DA	Migrado	Mediano	600
78	Sistema de Planeación de Recursos Institucionales II	TODAS	Migrado	Complejo	1200
79	Sistema de Planeación de Recursos Institucionales - Administración de Desempeño Empresarial (Enterprise Performance Management)	DF	Migrado	Complejo	1200
80	Sistema de Planeación de Recursos Institucionales (PREI)	DF	Migrado	Complejo	1200
81	Receta electrónica	DPM	Implementado inicialmente en centro de datos externo	Bajo	
82	Receta Seguimiento de Medicamento Específico	DPM	Implementado inicialmente en centro de datos externo	Bajo	
83	Reposición de Cédulas	DIR	Migrado	Bajo	300
84	Repositorio de Información Analítico	TODAS	Migrado	Mediano	600
85	Registro Nominal de Derechohabientes con Discapacidad	DPM	Migrado	Bajo	300
86	Consulta de Riesgos de Trabajo Terminados	DIR	Implementado inicialmente en centro de datos externo	Bajo	
87	Sistema de Administración de Bienes Muebles no Útiles y Desechos	DA	Migrado	Bajo	300

88	Sistema de Abasto Institucional Delegacional (SAI Farmacias)	DA	Migrado	Mediano	600
89	Sistema de Administración de Siniestros	DF	Implementado inicialmente en centro de datos externo	Mediano	
90	Sistema de Administración de Tiendas	DPES	Migrado	Bajo	300
91	Sistema de Control de Incapacidades	DPM	Migrado	Bajo	300
92	Sistema de Consulta para las Técnicas en Atención y Orientación al Derechohabiente (SCTAOD)	CAQOD	Migrado	Bajo	300
93	Servicio Digital de Productividad Médica	DPM	Implementado inicialmente en centro de datos externo	Mediano	
94	Servicio Digital de Recepción de Facturas para Proveedores	DF	Migrado	Mediano	600
95	Seguridata	DIR	Migrado	Mediano	600
96	Sistema Ejecutivo de Información	DA	Migrado	Bajo	300
97	Servicios Digitales de Pensiones	DPES	Implementado inicialmente en centro de datos externo	Complejo	
98	Repositorios Documentales (Sharepoint)	TODAS	Migrado	Mediano	600
99	Sistema de Información y Administración de Guarderías	DPES	Migrado	Mediano	600
100	Sistema de Información y Administración de Guarderías Central	DPES	Migrado	Mediano	600
101	Sistema Integral de Administración de Personal	DA	Migrado	Complejo	1200
102	Sistema Informático del Centro Automatizado de Distribución de Insumos Terapéuticos	DA	Migrado	Mediano	600
103	Sistema Institucional de Control de Gestión de Correspondencia	DA	Migrado	Complejo	1200
104	Sistema de Información de Convenios Internacionales	DPEI	Migrado	Bajo	300
105	Nuevo dictamen electrónico	DIR	Implementado inicialmente en centro de datos externo	Complejo	

106	Servicio de Identidad Electrónica IMSS Digital	DIR	Implementado inicialmente en centro de datos externo	Complejo	
107	Sistema de Información Médico Operativo Central	DPM	Implementado inicialmente en centro de datos externo	Bajo	
108	Servicio de Información de Mi Pensión Digital	DPES	Implementado inicialmente en centro de datos externo	Bajo	
109	Sistema de Notificación en Línea para la Vigilancia Epidemiológica	DPM	Migrado	Mediano	600
110	Sistema de Pago Referenciado	DIR	Migrado	Complejo	1200
111	Sistema de Préstamos Financieros con Entidades Externas	DPES	Migrado	Mediano	600
112	Sistema de Prestadores de Servicios	DIR	Migrado	Bajo	300
113	Sistema de Información de Prestaciones Sociales Institucionales	DPES	Migrado	Bajo	300
114	Sistema Institucional de Quejas Médicas	DJ	Migrado	Bajo	300
115	Sistema de Registro Electrónico de la Coordinación de Investigación en Salud	DPM	Migrado	Mediano	600
116	Sistema de Registro de Obras de la Construcción	DIR	Implementado inicialmente en centro de datos externo	Mediano	
117	Sistema de Corrección en Línea	DIR	Migrado	Mediano	600
118	Sistema de Certificación de Semanas Cotizadas a Solicitud del Asegurado	DIR	Implementado inicialmente en centro de datos externo	Mediano	
119	Sistema para Laboratorios	DPM	Migrado	Bajo	300
120	Sistema de Comprobación de Supervivencia	DPES	Migrado	Bajo	300
121	Sistema de Trámite de Pensiones	DPES	Migrado	Mediano	600
122	Sitio Web Institucional	TODAS	Migrado	Mediano	600
123	Servicio para Optimización de Procesos en Segundo y Tercer Nivel	DPM	Migrado	Mediano	600
124	Carpeta Electrónica de la Asamblea General y H. Consejo Técnico	SG	Migrado	Bajo	300

125	Sistema de Seguimiento de Consulta Ciudadana	DJ	Migrado	Bajo	300
126	Sistema de Trámite de Inscripción a Guardería por Internet	DPES	Migrado	Mediano	600
127	Sistema de Traslado de Pacientes	DF	Migrado	Bajo	300
128	Repositorio de Código Fuente (Team Foundation Server)	DIDT	Migrado	Mediano	600
129	Tablero de Información de Datos Abiertos Cifras del Empleo	DIR	Migrado	Mediano	600
130	App Móvil Tu Perfil IMSS	DA	Implementado inicialmente en centro de datos externo	Bajo	
131	Vales de Medicamentos	DA	Implementado inicialmente en centro de datos externo	Bajo	
132	Visor de solicitudes	DIR	Implementado inicialmente en centro de datos externo	Bajo	
133	Web Service de Certificación de Inactividad para el Pago de Parcialidades	DIR	Implementado inicialmente en centro de datos externo	Bajo	
134	Web Service de Certificación del derecho al Retiro por Desempleo	DIR	Migrado	Mediano	600
135	Sistema Integral de Medicina Familiar	DPM	Migrado	Mediano	600
136	Servicios de Inteenet	TODAS	Migrado	Mediano	600
137	Reclutamiento de Personal	DA	Migrado	Mediano	600
138	PREVENIMSS en su Empresa	DPM	Migrado	Bajo	300
139	CALL CENTER	TODAS	Migrado	Mediano	600
140	SAT	DIR	Migrado	Bajo	300
141	RENAPO	DIR	Migrado	Bajo	300
142	EDUTK	TODAS	Implementado inicialmente en centro de datos externo	Bajo	
143	Cita Médica Telefónica	DPM	Implementado inicialmente en centro de datos externo	Mediano	
144	TOOAD	DG	Implementado inicialmente en centro de datos	Mediano	

ANEXOS

DIVISIÓN DE CONTRATOS

			externo		
145	Micrositio Estar Bien Capacitación Virtual	DG	Implementado inicialmente en centro de datos externo	Bajo	
146	Seguimiento a Programas y Proyectos de la DA	DA	Implementado inicialmente en centro de datos externo	Bajo	
147	Riesgo de Cáncer	DA	Implementado inicialmente en centro de datos externo	Bajo	
149	Tienda Virtual	DA	Implementado inicialmente en centro de datos externo	Bajo	
150	Adquisición consolidada de medicamentos	DA	Implementado inicialmente en centro de datos externo	Bajo	
151	Componente de Seguridad de Control de Acceso a Aplicaciones	todas	Implementado inicialmente en centro de datos externo	Mediano	
152	Archivo Clínico Digital	DPM	Implementado inicialmente en centro de datos externo	Mediano	
153	Plataforma de Administración de Identidades	DIR	Migrado	Bajo	300
154	Micrositio de Arquitectita Tecnológica	DIDT	Implementado inicialmente en centro de datos externo	Bajo	
155	Modelo Preventivo de Enfermedades Crónicas	DPM	Implementado inicialmente en centro de datos externo	Mediano	

El proveedor deberá considerar los esfuerzos de migración no estimados, correspondientes a los sistemas que se implementaron desde inicio en el centro de datos actual.

El LICITANTE deberá ofertar en su propuesta económica el costo del concepto de migracion bajo el rubro "migración de centros de datos", incluyendo los tiempos de posible afectación a la

operación debido a los procesos de migración de información de los aplicativos, sistemas y servicios electrónicos o digitales del IMSS antes mencionados de manera enunciativa mas no limitativa, del Centro de Datos Actual a la infraestructura ofertada por el LICITANTE, tanto al interior del Instituto como con los Organismos con los que éste interopera, tales como Servicio de Administración Tributaria (SAT), Registro Nacional de Población (RENAPO), Comisión Nacional Para el Sistema de Ahorro para el Retiro (CONSAR), Infonavit, ProceSar, Afores, Bancos, Instituto Nacional Electoral (INE), entre otros, con los cuales el IMSS intercambia información e interopera procesos de negocio en su gran mayoría en línea o mediante procesos de bloques sincronizados, incluyendo los procesos de sincronización que se realizan diariamente entre los principales sistemas y servicios operados en el centro de datos administrado y el ecosistema IBM Mainframe ubicado en los centros de datos Institucionales, en los que se sincroniza diariamente la información de recaudación, vigencia de derechos, movimientos Afiliatorios y en general toda la sincronización entre los principales sistemas y aplicativos institucionales.

El proveedor deberá, como parte de la migración, garantizar la operación de los sistemas y aplicativos migrados de tal manera que operen con los mismos niveles de servicio que antes de ser migrados y con esto, el Instituto pueda mantener los Niveles de Atención de los servicios que presta a derechohabientes, patrones, pensionados, trabajadores del Instituto y público en general.

8. Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Ing. Héctor Javier Reyes Oropeza	Titular de la División de Administración, Procesamiento y Almacenamiento		12/11/2019
Lic. Carlos Francisco Ramirez Del Rivero	Titular de la División de Administración y Continuidad de la Operación		12/11/2019
Mtro. Hector Martinez Valenzuela	Titular de la División de Telecomunicaciones		12/11/2019
Mtro. Alejandro Paniagua Ramirez	Titular de la División de Administración de Riesgos Tecnológicos		12/11/2019

Revisó	Cargo	Firma	Fecha
Ing. Javier Cortés López	Titular de la Coordinación Técnica de Operación de Servicios Tecnológicos		12/11/2019
Ing. Carlos Calderon Zacarias	Titular de la Coordinación Técnica de Redes y Telecomunicaciones		12/11/2019

Aprobó	Cargo	Firma	Fecha
Ing. Eduardo Oropeza Ortíz	Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional		12/11/2019

Servicios de Continuidad de la Nube IMSS 2020

Apéndice #4. Relación actual de Infraestructura en Centro de Datos y proyección de crecimiento

Contenido

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	14/10/2019	Elaboración de documento	Ing. Héctor Javier Reyes Oropeza Lic. Carlos Francisco Ramírez del Rivero Ing. Héctor Martínez Valenzuela Ing. Alejandro Paniagua Ramírez
0.2	28/10/2019	Actualización del documento	Ing. Javier Cortés López Ing. Carlos Calderón Zacarías
1.0	12/11/2019	Aprobación del documento	Ing. Eduardo Oropeza Ortiz

ANEXOS

DIVISIÓN DE CONTRATOS

1. Objetivo del documento

El objetivo del presente Apéndice es dar a conocer a los licitantes las volumetrías que el Instituto consume a la fecha, así como las estimaciones de consumo para el año 20202, a fin de que cuente con elementos para el cálculo de la propuesta para la fase de migración del servicio administrado objeto de esta Licitación, para lo previsto en el Anexo Técnico correspondiente, apéndice, términos y condiciones, anexos, oferta del licitante, y documentación contractual.

La volumetría aquí señalada es de manera referencial y podrá ser distinta a la que se requiera al inicio del servicio..

2. Relación actual de Infraestructura

A continuación, se muestra una tabla que indica un estimado del uso de cada uno de los servicios al término de la vigencia del contrato actual.

Se deberá considerar que la infraestructura aquí señalada pertenece al último contrato celebrado con el instituto, por lo que la definición de infraestructura o características del servicio corresponden a las ofertas de Mercado de ese año.

El Licitante deberá considerar en su propuesta de servicio las conversiones a las características actuales del mercado.

	Cantidad
Servidor X86	724
Incrementos de Módulos de 1 Procesador con 128 threads X86	51
Incrementos de 128GB de memoria RAM X86	56
Módulo de Seguridad en Hardware (HSM)	1
Almacenamiento de Datos Individual INCREMENTOS VMAX	531
Incremento de Almacenamiento de Datos Individual de 100GB	4907
Respaldo de Datos Individual INCREMENTO DE DATADOMAIN 500GB	81
Unidad de almacenamiento de media categoría para aplicaciones de bajo desempeño VNX	2
Incremento en disco de estado sólido 1TB para almacenamiento bajo desempeño IVNX	1
Incremento en disco FC solido 1TB usable para almacenamiento bajo desempeño IVNX (SATA)	16
Unidad de respaldo de plataforma abierta	5
Incremento de bloques de 30TB usables en arreglo RAID 5 para unidades de plataforma abierta IDD	6
Unidad de Almacenamiento de Datos de alto rendimiento y red SAN VMAX CON SAN	1
Incremento en discos de estado sólido 1TB para almacenamiento de alto rendimiento IVMAX	8

Unidad individual de respaldos (Portatil)	505
Sistema Operativo Red Hat Enterprise Linux	22
Sistema Operativo SLES	11
Sistema Operativo Oracle Linux Server	447
Sistema Operativo Windows Server 2008	32
Sistema Operativo Windows 2012	4
Servidor Virtual RISC SPARC	7
Incremento de 1 Procesador Virtual con 128 threads RISC	4
Servidor Virtual X86 4VCPU 16 RAM	518
Incremento Virtualizado Módulos de 1 Procesador Virtual con 8 threads X86	411
Incremento Virtualizado 8GB de memoria RAM X86	506
Puntos de Acceso a la Nube	1306
Escritorio en la Nube	945
Plataforma de Virtualizacion multi-tecnologia	2
Punto Neutro	1
Conectividad de Enlaces MPLS 5 Gbps redundante activo - activo	3
Conectividad de Enlaces Lan2Lan 100 Mbps redundante activo - activo	1
UTM para enlaces de banda ancha hasta 100 Mbps	2
UTM para enlaces de banda ancha hasta 10 Gbps	2
Balanceador de carga de capas L4-L7	2
Plataforma Nodo de Extensión de Nube Privada - Tamaño grande	1
Piso Blanco	3
Espacio en Rack	1
Oracle Business Intelligence	30
Tableau Server	23
Tableau Desktop	23
Oracle ODI	11
Bases de Datos Oracle - StandAlone	2216
Bases de Datos Oracle - RAC	14
Microsoft SQL Server	1
Subscripciones a Bases de Datos Open Source	5
Liferay Enterprise 7/24	4
Liferay Enterprise 5/8	1
SOA Suite	15
WebLogic	1239
GlassFish	9

Apache Tomcat	1
Apache HTTPD	92
Oracle BPM	14
Servicio de correo electrónico.	79110
Firewall	6
IPS	1
Anti-Denegación de Servicios (DDoS)	1
Redes Privadas Virtuales - VPN	2
Gestión Unificada de Amenazas (UTM)	2
Filtrado de Contenido Web	1
Antispam	1
Antimalware	1
Firewall Especializado en Servicios Web (WAF)	1
Nodo de red con UTP	629
Nodo de red con Fibra Optica	64
Switch de 10G de core	16
Switch de 1G de distribución	70
UTM para enlaces a Red Nacional para Impulso de la Banda Ancha (NIBA) de 100 Mbps	2
Enlaces Internet 100 Mbps redundante activo - activo	2
Sistema de Almacenamiento de datos en RAID5 de 12TB con capacidad de crecimiento hasta 32TB	74
Solución para el cumplimiento WCAG	1

3. Descripción de conceptos según servicio actual de Centro de Datos

3.1 Servidor X86

El componente asociado al Servidor Físico x86 que consta de 1 o 2 procesadores y 128 GB en RAM, ofrece las siguientes características técnicas:
El Procesador deberá ser de al menos alguna de las siguientes familias:

- Intel® Xeon® Processor E5, E7 v3 o superior
  - Cache de 20MB a 45MB
  - Velocidad de 1.90GHz a 3.20GHz
- Intel® Xeon® Processor 7000 Sequence
  - Cache de 4MB a 24MB
  - Velocidad de 1.90GHz a 3.20GHz

Este componente considera los siguientes incrementos de capacidades:

- Incrementos de 128GB de memoria RAM x86
- Incrementos de Módulos de 1 Procesador

3.2 Módulo de Seguridad en Hardware (HSM)

Especificaciones del Módulo de Alta seguridad Criptográfica (HSM)
Niveles de Seguridad Mínimos

- Certificación FIPS 140-2 Nivel 3
- Common Criteria EAL 4+

Especificaciones Funcionales Mínimas

- Almacenamiento y procesamiento de llaves criptográficas
- Cifrado de llaves simétricas (DES, 3DES de dos y tres claves, SAFER, AES, ARIA, CAST) en modos:
  - ECB
  - CBC
  - CFB-64
  - OFC-64
- Hash (MD5, SHA-1, SHA-2, (224, 256, 384, 512), RIPEMD) en 128 y 160 bit
- Llaves RSA de hasta 4096 bits, Diffie-Hellman.
- Time Control
- Control de acceso multinivel autenticado
- Duty Segregation (Administrador y operador)
- Almacenamiento no limitado de llaves
- Generación de claves mediante random number generator de acuerdo a FIPS 186-2

Especificaciones Técnicas Mínimas

- Dos coprocesadores RSA
- Coprocesador simétrico
- Protección anti-tampering de la tarjeta HSM (sensores al menos para temperatura, acceso físico, tensión)
- Generación de números aleatorios por hardware
- Puertos Gigabit Ethernet
- Interfaz PCI 2.1

3.3 Almacenamiento de Datos Individual

Servicio de Almacenamiento de Datos con espacio inicial de 500 GB utilizables considerando el uso de RAID 5 o mejor.

Considera unidades de Incremento de Almacenamiento de Datos Individual de 100GB.

3.4 Respaldo de Datos Individual

Consiste en componentes tecnológicos que ofrecen el servicio para el sistema de respaldos de Datos con las siguientes características:

- Protección de tipo mínimo RAID 6
- Cuenta con conectividad FC y Ethernet, basada en discos SAS, con funciones de deduplicación interna y replicación vía enlace IP.
- Garantiza que la pérdida de un disco en la unidad de almacenamiento no genera la pérdida de información, ya que está configurada con una protección de al menos RAID 6.

3.5 Unidad de almacenamiento de media categoría para aplicaciones de bajo desempeño

Servicio de almacenamiento de media categoría para almacenar todo lo correspondiente a equipos virtualizados

3.6 Unidad de respaldo de plataforma abierta

Servicio de respaldo de aplicaciones desarrolladas en plataforma abierta, con las siguientes características:

- Capacidad base usable de almacenamiento de al menos 90TB con protección de tipo mínimo RAID 5
- Aprovechamiento de las redes de conectividad LAN y SAN, el almacenamiento debe contar con conectividad FC y Ethernet, basada en discos SAS, con funciones de deduplicación interna y replicación vía enlace IP.
- La pérdida de un disco en la unidad de almacenamiento no genera la pérdida de información, ésta deberá estar configurada con una protección de al menos RAID 6, con al menos un disco de hotspare.
- Garantizar la disponibilidad y su mantenimiento no disruptivo dando continuidad al servicio de respaldo y restauración.

Posibilidad de gestionar incrementos de bloques de 30TB usables en arreglo RAID 5 o superior para unidades de plataforma abierta

3.7 Unidad de Almacenamiento de Datos de alto rendimiento y red SAN VMAX CON SAN

Consiste en un servicio de almacenamiento de Datos de alto rendimiento y red SAN que cuenta con las siguientes características:

- Contar con al menos 2 switches de tipo director de por lo menos 384 puertos cada uno y que cada puerto sea de al menos 16 GBps.
- Contar con una capacidad base de almacenamiento de al menos 90TB utilizables con protección de tipo mínimo RAID 5
- Ser un almacenamiento de alta disponibilidad.
- Contar con tecnología de interconexión InfiniBand de 56 Gb/s.
- Considera la posibilidad de ejercer incremento en discos de estado sólido 1TB para almacenamiento de alto rendimiento

3.8 Unidad individual de respaldos (Portatil)

Servicio basado en equipos de unidad de respaldos portátil, el cual cuenta con las siguientes características mínimas:

- El procesador Intel Celeron Processor (2.58GHz, Dual-Core) o superior
- Memoria AGB DDR3L SODIMM o superior
- Disco duro: 3.5" SSD con una capacidad de almacenamiento de al menos 10 TB
- Fuente de poder de 100~240 V AC
- Soportar los siguientes sistemas de archivos: EXT4, FAT32, NTFS, HFS+ o equivalentes.

3.9 Sistema Operativo Red Hat Enterprise Linux

Servicios de administración de la plataforma RED HAT ENTREPRISE LINUX SERVER o equivalente según las necesidades del IMSS. El proveedor actual ejecuta las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Para este servicio se considerarán los Bloques de Construcción Fundamentales sobre el producto RED HAT ENTREPRISE LINUX SERVER, de acuerdo a lo que se especifica en el Apéndice correspondiente.
- Software de RED HAT ENTREPRISE LINUX SERVER o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 6 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.10 Sistema Operativo SLES

Servicios de administración de la plataforma SUSE LINUX ENTERPRISE SERVER o equivalente. Considera la ejecución las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos:

- Software de SUSE LINUX ENTERPRISE SERVER o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 10 y posteriores
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.11 Sistema Operativo Windows Server 2008

Servicios de administración de la plataforma Windows Server 2008 o equivalente según las necesidades del IMSS. El proveedor ejecuta las acciones necesarias para garantizar la continuidad de la operación.

3.12 Sistema Operativo Windows 2012

Servicios de administración de la plataforma Windows 2012 o equivalente según las necesidades del IMSS. El proveedor ejecuta las acciones necesarias para garantizar la continuidad de la operación.

3.13 Servidor Virtual RISC SPARC

Infraestructura virtual basada en RISC con procesador SPARC, que cumpla con algunas de las siguientes arquitecturas base:

- Oracle SPARC T5-8 Server
- SPARC T5 16-cores a 3.6 GHz
- 128 threads por procesador
- Cache 8 MB compartidos, Level 3 Cache; 128 KB Level 2
-

Bloque de construcción que habilita el incremento de capacidad de procesamiento de la máquina virtual basada en arquitectura RISC-SPARC.

3.14 Servidor Virtual X86 4VCPU 16 RAM

El componente asociado al Servidor Virtual x86 que consta de 4 vCPUs y 16 GB en RAM, ofrece las siguientes características técnicas:

El Procesador deberá ser de al menos alguna de las siguientes familias:

- Intel® Xeon® Processor E5, E7 v3 o superior
  - Cache de 20MB a 45MB
  - Velocidad de 1.90GHz a 3.20GHz
- Intel® Xeon® Processor 7000 Sequence
  - Cache de 4MB a 24MB
  - Velocidad de 1.90GHz a 3.20GHz

Este componente considera los siguientes incrementos de capacidades:

- Incremento Virtualizado 8GB de memoria RAM x86
- Incremento Virtualizado Módulos de 4 vCPUs

3.15 Puntos de Acceso a la Nube

Los Puntos de Acceso a la Nube (PAN) son estaciones de trabajo ligeras que se implementan bajo demanda y permiten el acceso a los servicios de la Nube IMSS, en especial a los EN, así como a la red del Instituto. Los PAN permiten el acceso a uno o varios usuarios (no simultáneo), por medio de un medio de identificación definido por el Instituto.

3.16 Escritorio en la Nube

Son escritorios de trabajo virtuales para clientes finales. El escritorio implementa las siguientes funcionalidades como parte integral del servicio:

- Escritorio de trabajo. Construcción del escritorio que incluye los Bloques de Construcción Fundamental que el Instituto determina en forma de Bloque de Construcción Común.
- Aprovisionamiento y bóveda de identidades. Funcionalidad de sincronización de identidades desde distintas fuentes y la generación del repositorio de identidades. Con esta funcionalidad el usuario consume su propia identidad en los sistemas asociados y usará el portal de colaboración del ENP para que restablezca su contraseña o solicitar nuevos permisos en los aplicativos.
- Control de acceso. Funcionalidad para controlar las identidades, proveer autenticación, autorización, y proveer un marco de trabajo para autenticación avanzada como por ejemplo biométricos, tarjetas inteligentes.

3.17 Plataforma de Virtualizacion multi-tecnologia

Para la habilitación de la Nube Privada, el IMSS cuenta con los servicios asociados a plataformas de virtualización que soporta las diferentes tecnologías virtualización para diferentes sistemas operativos.

Esta plataforma incluye todo el software y hardware, así como licencias de software, instalación, configuración, puesta a punto, soporte, operación, administración y todo lo necesario para su correcta implementación.

Soportar la creación y administración de máquinas virtuales así como la configuración de toda la solución conforme a lo requerido por el Instituto.

Gracias a este componente, el Instituto puede solicitar durante la vigencia del contrato servicios de virtualización solicitados para las tecnologías que tenga establecidas el Instituto en el repositorio de arquitectura de la Nube IMSS.

Cada plataforma soporta una capacidad de virtualización de hasta 800 cores x86 de procesamiento por cada tecnología de virtualización. La cantidad de Plataformas requeridas por el Instituto está asociada a la capacidad de procesamiento en Máquinas Virtuales existentes dentro el ecosistema tecnológico.

3.18 Punto Neutro

El Punto Neutro del IMSS es un modelo de telecomunicaciones para sirve para interconectar múltiples proveedores y múltiples tecnologías, formando una red híbrida, que se convierte en el Punto Neutro de comunicaciones. De esta manera las distintas necesidades del IMSS convergen permitiendo el crecimiento de servicios de transmisión de datos sin dependencias de un solo proveedor, con un marco tecnológico de conexión estandarizada, controlada y segura entre redes permitiendo tener una latencia optimizada.

3.19 Enlaces para conectividad de Red de Área Amplia e Internet

Para la entrega de los servicios que el Instituto ofrece a los derechohabientes y para garantizar la operación que el IMSS ejecuta a través de todo el ecosistema de salud y de oficinas administrativas que requiere para sustentar sus procesos de negocio, el IMSS requiere los siguientes elementos de conectividad que actualmente forman parte del contrato de Nube IMSS:

- Conectividad de Enlaces Lan2Lan 100 Mbps redundante activo - activo
- Conectividad de Enlaces MPLS 5 Gbps redundante activo - activo
- Enlaces Internet 100 Mbps redundante activo - activo

3.20 Balanceador de carga de capas L4-L7

Se cuenta con suministro de servicios de Balanceo L4-L7 para aplicaciones Web o equivalente y su información inherente altamente redundante. La infraestructura cumple con las siguientes especificaciones técnicas:

- Es de la familia:
  - BIG-IP 7000 Series
  - A10 3000 series
- Soporta los siguientes módulos:
  - Local Traffic Manager
  - Aceleración SSL

3.21 Plataforma Nodo de Extensión de Nube Privada - Tamaño grande

El nodo de Extensión de Nube Privada (ENP) es auto-contenido y tiene la capacidad de implementar acceso, seguridad, gestión y archivos, usar métodos de sincronización, conectividad o federación para conectarse con el centro de datos principal. Reduce el flujo de tráfico por la WAN entre el nodo de ENP y el centro de datos principal, aumentando la disponibilidad y mejorando la respuesta en sitios de mayor relevancia y demanda de la atención de servicios digitales y de información del Instituto.

Ofrece la capacidad de albergar al menos 8 Racks de 6.5KW

3.22 Piso Blanco

Consiste en el aprovechamiento de espacio físico dentro del Centro de Datos del proveedor, en unidades medidas por metro cuadrado, con la finalidad de poder alojar equipamiento propio o de otros proveedores externos en las instalaciones del proveedor.

3.23 Espacio en Rack

Consiste en el uso espacio en Rack en las instalaciones del proveedor de la Nube IMSS, con la finalidad de poder alojar equipamiento propio o de otros proveedores externos en las instalaciones del proveedor.

3.24 Oracle

Actualmente el instituto cuenta con diferentes componentes de Software del fabricante Oracle. Dichos elementos son provistos por el proveedor actual dentro de un esquema de servicios integrales que incluye el licenciamiento, los servicios de administración y soporte de fabricante, bajo un esquema de licenciamiento asociado al número de usuarios o cantidad de procesadores utilizados por la plataforma, según el esquema de licenciamiento definido por el fabricante. Los componentes de software Oracle que actualmente utiliza el instituto son:

- Bases de Datos Oracle – RAC
- Bases de Datos Oracle – StandAlone
- GlassFish
- Oracle BPM
- Oracle Business Intelligence
- Oracle ODI
- Sistema Operativo Oracle Linux Server
- SOA Suite
- WebLogic

3.25 Tableau Server

Los servicios de administración de la plataforma Tableau Server o equivalente.

Requerimientos Mínimos:

- Software de Tableau Server o equivalente (soporte empresarial)
- Versión 9 y posteriores del producto
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante
- Licenciamiento por cada 10 usuarios

3.26 Tableau Desktop

Servicios de administración de la plataforma Tableau Desktop o equivalente.
Requerimientos Mínimos

- Software de Tableau Desktop o equivalente (soporte empresarial)
- Versión 9 y posteriores del producto
- Soporte del producto por el fabricante 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante
- Licenciamiento por usuario

3.27 Microsoft SQL Server

Motor de Base de Datos Microsoft o equivalente de al menos las siguientes versiones: 2008 SP1 o superior.

Este servicio incluye el licenciamiento del producto así como el soporte y mantenimiento del mismo.

3.28 Subscripciones a Bases de Datos Open Source

Servicio de suscripción al uso de Bases de Datos Open Source.

Este servicio incluye el soporte y mantenimiento del producto.

Para la entrega de la Plataforma e Infraestructura de Bases de Datos OpenSource, el proveedor debe realizar las siguientes actividades:

- Instalar motores con la versión de acorde a lo solicitado por el comité de arquitectura y de acuerdo a las necesidades que el Instituto requiera.
- Considerar al menos las siguientes plataformas de Base de Datos opensource: PostgreSQL, MySQL, MongoDB, Cassandra DB.

- Crear, modificar y eliminar ambientes (Productivos, QA y Desarrollo) de acuerdo a las especificaciones que el Instituto determine (Unidades de Directorio).
- Evaluar el hardware para el servidor de base de datos con la finalidad verificar compatibilidad y garantizar que el producto pueda utilizar mejor los recursos informáticos disponibles como por lo menos unidades de disco para los productos de OpenSource, unidades de cinta dedicados disponibles, memoria disponible para las instancias de base de datos.
- Planear la estructura de almacenamiento lógico de la base de datos, el diseño general de la base de datos, la estrategia de la copia de seguridad, el rendimiento del servidor de base de datos y de la misma base de datos, durante las operaciones de acceso a datos, la eficiencia de los procedimientos de respaldo y recuperación, la planificación del diseño relacional de los objetos de la base y las características de almacenamiento para cada uno de estos objetos, mediante la planificación de la relación entre cada uno y su almacenamiento físico antes de crearlo.

3.29 Liferay Enterprise

Servicios de administración de la plataforma Content Management LIFERAY ENTERPRISE o equivalente según las necesidades. El proveedor deberá ejecutar las acciones necesarias para garantizar la continuidad de la operación.
Requerimientos Mínimos:

- Software de Content Management LIFERAY ENTERPRISE Support o equivalente (soporte empresarial que incluye Indemnización legal)
- Versión del producto 6.0 y posteriores
- Soporte del producto por el fabricante 5/8 o 7/24, en modalidad remota, en línea y presencial en las instalaciones del Instituto
- Actualización y parches (releases/bugfixes)
- Acceso a bases de conocimientos del fabricante

3.30 GlassFish

Administración de la plataforma GLASSFISH o equivalente según sean sus necesidades. Incluye las acciones necesarias para garantizar la continuidad de la operación.

3.31 Apache Tomcat

Servicios de administración de la plataforma Apache Tomcat o equivalente según las necesidades del IMSS. Incluye las acciones necesarias para garantizar la continuidad de la operación.

3.32 Apache HTTPD

Servicios de administración de la plataforma Apache HTTPD o equivalente según las necesidades del IMSS. Incluye las acciones necesarias para garantizar la continuidad de la operación.

3.33 Servicio de correo electrónico

Servicio de administración del correo electrónico corporativo durante la vigencia del contrato.

Incluye todas las acciones necesarias para garantizar la continuidad de la operación y seguridad de la información.

3.34 Firewall

La funcionalidad de Firewall entrega servicios de seguridad y protección de control de acceso, bloqueo contra ataques dirigidos a las aplicaciones e inspección sobre los paquetes a nivel de aplicación para identificar patrones de tráfico anómalo desde y hacia la infraestructura que alberga los servicios del Instituto.

3.35 IPS

El servicio de IPS es responsable de la protección perimetral basada en firmas e identifica vulnerabilidades, para contener los intentos de obtener acceso a los recursos o servicios publicados en Internet o Intranet que pudieran afectar la operación del Instituto. Este componente permite detectar accesos no autorizados y previentes fugas de información.

3.36 Anti-Denegación de Servicios (DDoS)

El Instituto cuenta con un servicio de protección contra ataques de Denegación de Servicio Distribuido basados en firmas para altos volúmenes de conexión. A través de este servicio el proveedor emite alertas de incidentes y monitorea los eventos generados por los elementos tecnológicos de la solución de Anti-denegación de Servicios (DDoS) relacionados.

Este servicio está implementado tanto en el Punto Neutro como en los inmuebles del instituto donde se suministran servicios de enlaces MPLS.

3.37 Redes Privadas Virtuales – VPN

Los enlaces de comunicaciones hacia los diferentes nodos de la red son parte de un servicio basado en la transmisión de información sobre el protocolo IP- que permite la implementación de redes privadas virtuales para comunicar a los diferentes puntos de una organización de manera segura y confiable, contando con la capacidad de diferenciar los tipos de información transmitida -como voz, datos y video- para proporcionar diferentes niveles de prioridad o tratamiento a cada uno de ellos (Quality of Service/Class of Service).

3.38 Gestión Unificada de Amenazas (UTM)

Los UTM son plataformas que entregan servicios de protección perimetral especializada en antivirus, antispyware, antispam, control de acceso, prevención de intrusos, Filtrado de Contenido Web y VPN, para control de tráfico y detección de actividad anómala, a través de un solo dispositivo que ofrece dichas capacidades de manera integral. Actualmente el instituto cuenta con diferentes tipos de equipos UTM, cuya principal diferencia es el rendimiento que ofrece respecto a la capacidad de análisis de tráfico para distintos anchos de banda. Los que se tienen dentro del ecosistema de la Nube IMSS son:

- UTM para enlaces de banda ancha hasta 100 Mbps
- UTM para enlaces a Red Nacional para Impulso de la Banda Ancha (NIBA) de 100 Mbps
- UTM para enlaces de banda ancha hasta 10 Gbps

ANEXOS

DIRECCIÓN DE CONTRATOS

3.39 Filtrado de Contenido Web

Permite controlar y filtrar la utilización de servicios de acceso a Internet desde los equipos de cómputo que operan en los inmuebles del instituto, mediante el establecimiento de políticas de acceso que permiten controlar el uso de dichos servicios, en función de roles y perfiles de los usuarios.

3.40 Antispam

El servicio de Antispam permite llevar a cabo el análisis de correos electrónicos de entrada y salida con el objetivo de bloquear amenazas de spam, malware, phishing, amenaza persistente avanzada (Advanced Persistent Threat APT's), reputación de URLs embebidas en los buzones de correo electrónico del Instituto.

3.41 Antimalware

El servicio de Antimalware (anti-malware) está diseñado para prevenir, detectar y remediar software malicioso en los dispositivos informáticos individuales y sistemas TI del Instituto para protección contra amenazas avanzadas de la red interna. Dicho servicio incluye de manera integral los servicios de instalación, operación y soporte; tanto para la infraestructura ubicada en el Centro de Datos como en los inmuebles donde el Instituto requiere dicha funcionalidad.

3.42 Firewall Especializado en Servicios Web (WAF)

Componente que entrega servicios de protección, prevención y control de ataques para aplicativos Web expuestos en Internet. Este servicio permite proteger los servidores de aplicaciones web del Instituto de determinados ataques específicos en Internet. El servicio previene los siguientes tipos de ataques:

- Cross-site scripting que consiste en la inclusión de código script malicioso en el cliente que consulta algún servidor web del Instituto.
- SQL injection que consiste en introducir un código SQL que vulnere la Base de Datos de servidiores del Instituto.
- Denial-of-service que consiste en que el servidor de aplicación sea incapaz de servir peticiones correctas de usuarios.

3.43 Nodo de red con UTP

Infraestructura de conectividad física basada en conectores de cobre tipo UTP categoría 6 o superior, rematados en un rack con panel de parcheo y conectores tipo face-plate. No incluye el tendido de cableado.

3.44 Nodo de red con Fibra Optica

Infraestructura de conectividad física basada en conectores de fibra óptica rematados en un rack con panel de parcheo y conectores tipo face-plate. No incluye el tendido de cableado.

3.45 Switch de 10G de core

Componente de conectividad LAN de alto rendimiento y alta modularidad. Se utilizan en las arquitecturas de conectividad del Instituto que requieren alto desempeño y capacidades de conectividad equivalentes a los 10 Gigabit Ethernet

3.46 Switch de 1G de distribución

Componente de conectividad LAN de alto rendimiento y alta modularidad. Se utilizan en las arquitecturas de conectividad del Instituto que requieren alto desempeño y capacidades de conectividad equivalentes a 1 Gigabit Ethernet.

3.47 Sistema de Almacenamiento de datos en RAID5 de 12TB con capacidad de crecimiento hasta 32TB

El servicio incluye la infraestructura para cumplir con el requerimiento del Instituto para contar con 12TB utilizables. Los gastos de instalación y configuración están considerados en el cálculo del precio mensual.

Consta de un sistema de almacenamiento de datos que puede ser dedicado o compartido. Para el caso de un equipo dedicado 100% al Instituto los aspectos de seguridad a considerar son los aspectos físicos en cuanto a accesos, cerraduras, controles varios, etc. Para el caso de equipo compartido, se debe asegurar, además de los aspectos físicos, que ninguno de los elementos de hardware asignados pueda ser accedido por personas ajenas al Instituto y que no tengan que ver con la administración del mismo, por ende se entiende que tampoco habrá acceso a la información del Instituto por parte de dichas personas.

3.48 Solución para el cumplimiento WCAG

Componente que permite al IMSS el contar con herramientas que permiten agregar funcionalidades de accesibilidad al contenido digital para sus derechohabientes y cumplir con las obligaciones en la materia. Este servicio se enfoca únicamente en la accesibilidad digital y se esfuerza continuamente por la innovación que permite al Instituto obtener los beneficios del contenido web completo y abierto.

4. Proyección de crecimiento

Descripción	Cantidad	
	2019	2020
Servidor X86	724	724
Incrementos de Módulos de 1 Procesador con 128 threads X86	51	51
Incrementos de 128GB de memoria RAM X86	56	56
Módulo de Seguridad en Hardware (HSM)	1	1
Almacenamiento de Datos Individual INCREMENTOS VMAX	531	531
Incremento de Almacenamiento de Datos Individual de 100GB	4907	4907

ANEXOS
DIVISIÓN DE CONTRATOS

Respaldo de Datos Individual INCREMENTO DE DATADOMAIN 500GB	81	81
Unidad de almacenamiento de media categoría para aplicaciones de bajo desempeño VNX	2	2
Incremento en disco de estado sólido 1TB para almacenamiento bajo desempeño IVNX	1	1
Incremento en disco FC solido 1TB usable para almacenamiento bajo desempeño IVNX (SATA)	16	16
Unidad de respaldo de plataforma abierta	5	5
Incremento de bloques de 30TB usables en arreglo RAID 5 para unidades de plataforma abiert IDD	6	6
Unidad de Almacenamiento de Datos de alto rendimiento y red SAN VMAX CON SAN	1	1
Incremento en discos de estado sólido 1TB para almacenamiento de alto rendimiento IVMAX	8	8
Unidad individual de respaldos (Portatil)	505	505
Sistema Operativo Red Hat Enterprise Linux	22	22
Sistema Operativo SLES	11	11
Sistema Operativo Oracle Linux Server	447	447
Sistema Operativo Windows Server 2008	32	32
Sistema Operativo Windows 2012	4	4
Servidor Virtual RISC SPARC	7	7
Incremento de 1 Procesador Virtual con 128 threads RISC	4	4
Servidor Virtual X86 4VCPU 16 RAM	518	518
Incremento Virtualizado Módulos de 1 Procesador Virtual con 8 threads X86	411	411
Incremento Virtualizado 8GB de memoria RAM X86	506	506
Puntos de Acceso a la Nube	1306	1306
Escritorio en la Nube	945	945
Plataforma de Virtualizacion multi-tecnologia	2	2
Punto Neutro	1	1
Conectividad de Enlaces MPLS 5 Gbps redundante activo - activo	3	3
Conectividad de Enlaces Lan2Lan 100 Mbps redundante activo - activo	1	1
UTM para enlaces de banda ancha hasta 100 Mbps	2	2
UTM para enlaces de banda ancha hasta 10 Gbps	2	2
Balanceador de carga de capas L4-L7	2	2
Plataforma Nodo de Extensión de Nube Privada - Tamaño grande	1	1
Piso Blanco	3	3
Espacio en Rack	1	1
Oracle Business Intelligence	30	30
Tableau Server	23	23

Tableau Desktop	23	23
Oracle ODI	11	11
Bases de Datos Oracle - StandAlone	2216	2216
Bases de Datos Oracle - RAC	14	14
Microsoft SQL Server	1	1
Subscripciones a Bases de Datos Open Source	5	5
Liferay Enterprise 7/24	4	4
Liferay Enterprise 5/8	1	1
SOA Suite	15	15
WebLogic	1239	1239
GlassFish	9	9
Apache Tomcat	1	1
Apache HTTPD	92	92
Oracle BPM	14	14
Servicio de correo electrónico.	79110	79110
Firewall	6	6
IPS	1	1
Anti-Denegación de Servicios (DDoS)	1	1
Redes Privadas Virtuales - VPN	2	2
Gestión Unificada de Amenazas (UTM)	2	2
Filtrado de Contenido Web	1	1
Antispam	1	1
Antimalware	1	1
Firewall Especializado en Servicios Web (WAF)	1	1
Nodo de red con UTP	629	629
Nodo de red con Fibra Optica	64	64
Switch de 10G de core	16	16
Switch de 1G de distribución	70	70
UTM para enlaces a Red Nacional para Impulso de la Banda Ancha (NIBA) de 100 Mbps	2	2
Enlaces Internet 100 Mbps redundante activo - activo	2	2
Sistema de Almacenamiento de datos en RAID5 de 12TB con capacidad de crecimiento hasta 32TB	74	74
Solución para el cumplimiento WCAG	1	1

ANEXOS

DIVISIÓN DE CONTRATOS

5. Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Ing. Héctor Javier Reyes Oropeza	Titular de la División de Administración, Procesamiento y Almacenamiento		12/11/2019
Lic. Carlos Francisco Ramirez Del Rivero	Titular de la División de Administración y Continuidad de la Operación		12/11/2019
Mtro. Hector Martinez Valenzuela	Titular de la División de Telecomunicaciones		12/11/2019
Mtro. Alejandro Paniagua Ramirez	Titular de la División de Administración de Riesgos Tecnológicos		12/11/2019

Revisó	Cargo	Firma	Fecha
Ing. Javier Cortés López	Titular de la Coordinación Técnica de Operación de Servicios Tecnológicos		12/11/2019
Ing. Carlos Calderon Zacarias	Titular de la Coordinación Técnica de Redes y Telecomunicaciones		12/11/2019

Aprobó	Cargo	Firma	Fecha
Ing. Eduardo Oropeza Ortíz	Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional		12/11/2019

Servicios de Continuidad de la Nube IMSS 2020

Apéndice #5. Especificaciones Técnicas de Seguridad de la Información

ANEXOS
DIVISIÓN DE CONTRATOS

Contenido

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	14/10/2019	Elaboración de documento	Ing. Héctor Javier Reyes Oropeza Lic. Carlos Francisco Ramírez del Rivero Ing. Héctor Martínez Valenzuela Ing. Alejandro Paniagua Ramírez
0.2	28/10/2019	Actualización del documento	Ing. Javier Cortés López Ing. Carlos Calderón Zacarías
1.0	12/11/2019	Aprobación del documento	Ing. Eduardo Oropeza Ortiz

ANEXOS
DIVISIÓN DE CONTRATOS

1. Objetivo del documento

El objetivo del presente Apéndice es establecer las especificaciones y características técnicas para los Bloques de Construcción Fundamentales y servicios asociados a la seguridad de la información para el servicio Administrado objeto de esta Licitación.

2. Especificaciones para los Bloques de Construcción Fundamentales Consideraciones

2.1.1 Firewall

Cumplir con al menos las siguientes funcionalidades operativas:

- Red perimetral con 7 zonas, Web, App, DB, Transversales, Monitoreo, Respaldo y Operación, entre otras.
- Incluir interfaces 10GigaEthernet
- Desempeño de 18Gbps y 2,000,000 conexiones concurrentes
- Capacidad de 150,000 nuevas conexiones por segundo
- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
- Certificado por organismos de la industria como Common Criteria o ICSA Labs.
- Incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permitir implementar reglas aplicadas a intervalos de tiempo específicos.
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
- Soportar y operar bajo protocolos de ruteo BGP y OSPF.
- Soportar y operar mediante rutas estáticas.
- Realizar inspección en capa 3 y 4.
- Integrar esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Capaz de establecer túneles VPN IPSEC/SSL con las siguientes características y especificaciones:
    - Deberá soportar DES, 3DES y AES-256 para las fases I y II de IKE.
    - Deberá soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
    - Deberá soportar integridad de datos con md5, sha1 y sha2.
    - Deberá soportar las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
    - Deberá soportar VPNs client-to-site basadas en IPSEC.
    - Deberá establecer VPNs con gateways con direcciones IP dinámicas públicas.
    - Deberá crear una única asociación de seguridad (SA) por par de redes o subredes.

  - Deberá realizar VPNs SSL.
  - Deberá soportar Secure Sockets Layer (SSL) versión 3, con al menos los siguientes algoritmos de cifrado simétrico y longitud de llaves: RC4 (128 bits) y 3DES (192bits).
  - Deberá soportar la conexión de dispositivos móviles a través de un cliente de acceso remoto específico. Dicho cliente debe soportar al menos las siguientes plataformas: MAC OS X desde v10.4.10, iOS desde v4, Android desde v4.2, Windows desde v7, BlackBerry OS desde v5.0
- Administración del sistema vía Web (HTTPS), por línea de comando (SSH), SNMPv3 y a través de una consola central de administración.
- Contar y operar al menos con una interface Gigabit Ethernet dedicada para administración.
- Generación de logs de múltiples niveles de criticidad.
- Incluir una consola centralizada de gestión con las siguientes características:
  - Configuración, de manera centralizada, de políticas en todos los firewalls de la infraestructura.
  - Inspección de tráfico por medio del firewall en la capa de aplicación.
  - Identificación de qué reglas corresponden a fuentes, destinos y tipos de tráfico.
  - Ejecución de operaciones para grupos o bloques de dispositivos de frontera de seguridad.
  - Capacidad de ofrecer diferentes vistas durante el monitoreo de dispositivos, topologías o políticas.
  - Agrupación de parámetros de configuración para su posterior implementación.
  - Durante una actualización de configuración, debe ser capaz de regresar a la configuración anterior, si es necesario o requerido.
- Capacidad de asignar el control adecuado a diferentes administradores, como mínimo, en cuatro (4) niveles de acceso.

2.1.2 IPS

El Licitante del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Soporte de al menos: 1,000,000 conexiones simultáneas por cada Gigabit de inspección.
- Latencia máxima de 0.5 milisegundos.
- Soporte de interfaces de 1GE y 10GE
- Deberá operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
- Capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado.
- Capacidad de detección en línea sin bloquear tráfico (Modo transparente). El sistema sólo alertará que eventos serían bloqueados.
- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.
- Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
- Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.
- La solución de IPS deberá contemplar que el flujo de información esté asegurado ante una falla en el IPS, pudiendo conmutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.

- Soporte de funcionalidades de alta disponibilidad y configuraciones del tipo activo/activo y activo/failover. Esto debe ser soportado sin degradar el desempeño del IPS y manteniendo las tasas de transmisión requerida.
- Soporte de actualizaciones automáticas de seguridad del archivo de firmas de cuando menos dos veces por mes.
- Soporte de análisis de tráfico de voz sobre IP.
- Soporte de monitoreo de VLANs, incluyendo tramas 802.1q
- Soporte de monitoreo de IPv6.
- Soporte de monitoreo con inspección profunda de paquete y monitoreo de paquete en escenarios de alta disponibilidad y con handshake TCP incompleto.
- Reconocimiento de Tuneleo de Protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
- Detección de re-ensamblaje de paquetes fragmentados.
- Captura de tráfico para el análisis de evidencia en formato soportado por TCPDUMP y de manera opcional en formato .ENC (estándar para el software de análisis de protocolos), dicho archivo podrá ser usado para hacer playback del ataque.
- Integración de Listas Blanca (IP whitelist) mediante una lista de direcciones IP "confiables" que el sistema no bloqueará.
- Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos host de la red y crear una alarma cuando cierto umbral sea rebasado.
- Capacidad de integración con el directorio de usuarios (Active Directory y/o LDAP).
- Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
- Administración de seguridad centralizada que incluya las políticas, actualización, respuestas (bloquear, notificar, ignorar, etc.) y opciones de auditoria.
- Consola centralizada que administre los IPSs y la integración de usuarios que realice las configuraciones necesarias para remediación de incidentes de seguridad.
- Consola remota con interfaz gráfica.
- Consola remota Web cifrada (HTTPS) en formato gráfico para el uso en modo de consulta.
- Perfiles diferentes de usuarios.
- Auditoria de las siguientes actividades de los usuarios: Inicio de sesión de usuarios, políticas instaladas en los sensores y tareas administrativas sobre los agentes

2.1.3 Anti-denegación de Servicios (DDoS)

El Licitante del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Basado en equipo de propósito específico (Hardware Appliance).
- Plataforma modular que permita escalar el desempeño de la solución.
- Deberá garantizar el paso transaccional de datos legítimos.
- Detección del tráfico basado en el lenguaje TCPDUMP (con información definida en las capas 3 y 4)
- Capacidad de advertir anticipadamente algún posible ataque, analizando tendencias de tráfico malicioso en tiempo real.
- Capacidad de monitoreo en tiempo real de los circuitos dedicados que entregan la conectividad a Internet para detectar el comportamiento anormal del tráfico que pueda estar dirigido a atacar las interfaces de los enrutadores implicados en el enlace.

- Capacidad de monitoreo en tiempo real las subredes pública que conectan los enlaces, para que permita la detección de tráfico anormal que pueda significar un ataque dirigida a ella.
- Detección de ataques basado en la línea de base contra los recursos definidos, con opciones configurables por recursos que permitan filtrar la sensibilidad de la anomalía y disparar una alarma, en paquetes por segundo y Mbps.
- Deberá monitorear de manera enunciativa más no limitativa las siguientes variables en tiempo real:
    - Para el protocolo IP:
        - icmp
        - Paquetes IP fragmentados
        - Paquetes IP NULL
        - Paquetes IP con direcciones privadas
    - Para el protocolo TCP:
        - Segmentos TCP NULL
        - Segmentos TCP RST
        - Segmentos SYN
    - Tráfico total
- Deberá como mínimo detectar los siguientes tipos de ataques DoS/DDoS sobre las interfaces, subredes y activos de infraestructura:
    - ACK Flood
    - SYN Flood
    - Hogging CPU
    - Chargen (Character generator)
    - FIN Flood
    - ToS Flood
    - DNS Malformed
    - HTTP Flood
    - ICMP Flood
    - UDP Flood
    - Non- UDP/TCP/ICMP Protocol Flood
    - PPS Flood Attack
    - Zombie attack
    - Land Attack
- Deberá de permitir la personalización de los niveles de alarma o umbrales que sirvan para la detección de ataques, a una granularidad por objeto monitoreado.
- Deberá monitorear actividad sospechosa que pueda significar algún ataque de gusanos o "Worms" o virus.
- Deberá monitorear actividad "Dark IP".
- Detección de anomalías DDoS y amenazas de día cero antes de que impacten en los servicios.
- Detección de zombis (con selecciones de umbrales en Mbps y pps desde el portal Web del cliente) para clasificar una IP como zombis y con la opción de conocer una lista de zombis activos detectados.
- Protección contra amenazas conocidas
    - Ping de la muerte
    - Ataque por inundación SYN
    - Fragmentación de paquetes y reensamblaje
    - Broadcast de correo electrónico
    - Saturadores de CPU

ANEXOS

- Scripts generadores de trafico
- Generadores de caracteres
- Ataques fuera de banda (WinNuke)
- Ataque Smurf (generador de gran cantidad de paquetes ICMP)

2.1.4 Redes Privadas Virtuales – VPN (C2S – S2S)

El Licitante del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Deberá incluir al menos 6 interfaces 10GE
- Deberá tener un desempeño de al menos 4Gbps y 1,000,000 conexiones concurrentes
- Capacidad de 50,000 nuevas conexiones por segundo
- Capacidad para incluir un sistema operativo endurecido propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Capacidad para incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Deberá permitir implementar reglas aplicadas a intervalos de tiempo específicos.
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Capacidad para integrar esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
- Deberá soportar DES, 3DES y AES-256 para las fases I y II de IKE.
- Soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Soportar integridad de datos con md5, sha1 y sha2.
- Soportar las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Establecer VPNs con gateways con direcciones IP dinámicas públicas.
- Crear una única asociación de seguridad (SA) por par de redes o subredes.
- Capacidad para realizar VPNs SSL.
- Capacidad para soportar Secure Sockets Layer (SSL) versión 3, con al menos los siguientes algoritmos de cifrado simétrico y longitud de llaves: RC4 (128 bits) y 3DES (192bits).
- Deberá soportar la conexión de dispositivos móviles a través de un cliente de acceso remoto específico. Dicho cliente debe soportar al menos las siguientes plataformas: MAC OS X desde v10.4.10, iOS desde v4, Android desde v4.2, Windows desde v7, BlackBerry OS desde v5.0
- Administración del sistema debe ser vía Web (HTTPS), por línea de comando (SSH), SNMPv3 y a través de una consola central de administración.
- Contar y operar al menos con una interface Gigabit Ethernet dedicada para administración.
- Generación de logs de múltiples niveles de criticidad.
- Incluir una consola centralizada de gestión con las siguientes características:
  - Configuración, de manera centralizada, de políticas en todos los firewalls de la infraestructura.
  - Inspección de tráfico por medio del firewall en la capa de aplicación.
  - Identificación de qué reglas corresponden a fuentes, destinos y tipos de tráfico.

- Ejecución de operaciones para grupos o bloques de dispositivos de frontera de seguridad.
- Capacidad de ofrecer diferentes vistas durante el monitoreo de dispositivos, topologías o políticas.
- Agrupación de parámetros de configuración para su posterior implementación.
- Durante una actualización de configuración, debe ser capaz de regresar a la configuración anterior, si es necesario o requerido.

- Capacidad de asignar el control adecuado a diferentes administradores, como mínimo, en cuatro (4) niveles de acceso.

2.1.5 Gestión Unificada de Amenazas (UTM)

El Licitante del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- UTM Tipo 1
  - Deberá incluir al menos 4 interfaces Ethernet de 10/100/1000 Mbps.
  - Deberá tener un desempeño de al menos 5Gbps y 4000 conexiones concurrentes.
  - Capacidad de 150,000 nuevas conexiones por segundo
  - Deberá incluir un sistema operativo endurecido propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- UTM Tipo 2
  - Deberá incluir al menos 4 interfaces Ethernet de 10/100/1000 Mbps.
  - Deberá tener un desempeño de al menos 10Gbps y 100,000 conexiones concurrentes.
  - Capacidad de 1,000,000 nuevas conexiones por segundo
  - Deberá incluir un sistema operativo endurecido propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Funcionalidad Firewall
  - Basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
  - Certificado por organismos de la industria como Common Criteria o ICSA Labs.
  - Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
  - Capacidad para permitir implementar reglas aplicadas a intervalos de tiempo específicos.
  - Deberá soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
  - Soportar y operar bajo protocolos de ruteo BGP y OSPF.
  - Soporte y operar mediante rutas estáticas.
  - Capacidad para realizar inspección en capa 3 y 4.
- Funcionalidad IPS
  - Soporte de al menos: 1,000,000 conexiones simultáneas por cada Gigabit de inspección.
  - Latencia máxima de 0.5 milisegundos.
  - Deberá operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
  - El equipo deberá ser capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado

ANEXOS

- Capacidad de detección en línea sin bloquear tráfico (Modo transparente). El sistema sólo alertará que eventos serían bloqueados.
- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.
- Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
- Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.
- La solución de IPS deberá contemplar que el flujo de información esté asegurado ante una falla en el IPS, pudiendo conmutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.
- Reconocimiento de Tuneleo de Protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
- Detección de re-ensamblaje de paquetes fragmentados.
- Integración de Listas Blanca (IP whitelist) mediante una lista de direcciones IP "confiables" que el sistema no bloqueará.
- Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos host de la red y crear una alarma cuando cierto umbral sea rebasado.

• Funcionalidad Filtrado de Contenido Web
  - Deberá permitir operar en modo de proxy explicito y/o proxy transparente.
  - Controlar e inspeccionar al menos los protocolos: HTTP, HTTPS (SSL).
  - Catalogar las páginas por Dominio (o subdominio), URL o IP.
  - Permitir personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
  - Permitir la creación de categorías de filtrado personalizadas así como la creación de listas blancas y negras de filtrado URL.
  - Capacidad de evitar la ejecución de códigos maliciosos.
  - Permitir el bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.
  - Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).

• Funcionalidad VPN
  - Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
  - Deberá permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
  - Capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
  - Deberá soportar DES, 3DES y AES-256 para las fases I y II de IKE.
  - Deberá soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
  - Deberá soportar integridad de datos con md5 y sha1.
  - Deberá soportar las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
  - Deberá establecer VPNs con gateways con direcciones IP dinámicas públicas.
  - Deberá crear una única asociación de seguridad (SA) por par de redes o subredes.

- Deberá soportar Secure Sockets Layer (SSL) versión 3, con al menos los siguientes algoritmos de cifrado simétrico y longitud de llaves: RC4 (128 bits) y 3DES (192bits).

2.1.6 Filtrado de Contenido Web

Soportar al menos las siguientes configuraciones para los procesos de autorización y autenticación:

- Integración con esquemas de autenticación provistas por el Instituto (DA, IDM, entre otras).
- Integración, mediante LDAP, con el directorio del Instituto para realizar la autenticación.
- Integración, mediante ICAP, con el servicio de filtrado Web del Instituto.

Gestionar los perfiles de navegación con base en las políticas de navegación del Instituto.

Gestionar la navegación de los usuarios del Instituto con base en las políticas y perfiles de acceso que apliquen.

Proteger contra el acceso inadvertido a sitios potencialmente peligrosos.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el Licitante del servicio deberá realizar la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

El Licitante del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Soportar de forma mínima 120,000 usuarios en esquema de alta disponibilidad.
- Permitir operar en modo de proxy explicito y/o proxy transparente.
- Mecanismos de autenticación tales como: archivos locales de contraseña NTLM, LDAP, RADIUS, Active Directory y certificados.
- Control de autenticaciones simultáneas con una misma cuenta de usuario.
- Cifrado de datos (usuario/contraseña) en el proceso de autenticación.
- Controlar e inspeccionar al menos los protocolos: HTTP, HTTPS (SSL), FTP, CIFS, MAPI, DNS, P2P, SOCKS (v4/v5), IM (AOL, MSN, Yahoo Messengers), TCP-Tunnel, MMS, RTSP.
- Catalogar las páginas por Dominio (o subdominio), URL o IP.
- Bloqueo de las amenazas emergentes más comunes como: pop-ups, banners, spyware, adware, compartición de archivos punto a punto (P2P file sharing).
- Catalogación en tiempo real de sitios en internet (on-the-fly) que aún no han sido asignados a alguna categoría (servicio automático de validación en línea del sitio para determinar si es malicioso en caso de no tenerlo asignado en alguna categoría).
- Monitoreo y bloqueo de aplicaciones P2P tales como: BitTorrent, eDonkey, Gnutella, Fasttrack.
- Permitir personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
- Permitir la categorización de URL en más de una categoría.
- Permitir el uso de expresiones regulares.
- Permitir la creación de categorías de filtrado personalizadas así como la creación de listas blancas y negras de filtrado URL.

- Capacidad de evitar la ejecución de códigos maliciosos.
- Bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.
- Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).
- Permitir la recopilación (caching) de páginas web en disco duro y memoria RAM, con el fin de hacer más eficiente el uso de los recursos del equipo.
- Proporcionar capacidades de administración y reporteo centralizado incluyendo control de acceso discrecional, control de versiones, auditoria de usuario, sistema y utilerías de restauración de configuración.
- Deberá proporcionar soporte de administración multisesión (múltiples administradores utilizando el servicio de administración centralizado), a través de una interfaz gráfica vía Web cifrada (HTTPS).

2.1.7 Antispam

El Licitante del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Capacidad de revisar tanto el correo entrante como el saliente.
- Contar con un filtro de contenido para buscar palabras clave en el cuerpo del mensaje, en los encabezados From, To, CC, Subject y en X-Headers. Así mismo, deberá poder detectar estas palabras en archivos adjuntos.
- Capacidad para poder configurar el tamaño máximo del mensaje y el número de destinatarios del correo tanto a nivel de conexión SMTP como en políticas cuando el correo ya ha sido recibido.
- Contar con mecanismos para clasificar los remitentes por su origen y tomar decisiones de flujo y volumen en consecuencia. Además se debe contar con la facilidad de designar ciertas fuentes de correo en grupos como listas negras, listas blancas o cualquier otro grupo al que deba aplicársele una política específica.
- Capacidad para ofrecer el análisis de archivos comprimidos en los formatos más populares, incluyendo aquellos con 7 capas de compresión.
- Capacidad de detectar el verdadero formato de un archivo y permitir aplicar políticas basadas en este rubro.
- Capacidad para detectar enlaces maliciosos dentro de los correos recibidos en base a la reputación de la URL, utilizando la tecnología de reputación del Fabricante, permitiendo la configuración de umbrales para esta detección.
- Contar con un módulo de bloqueo de correo electrónico no deseado con base en la reputación de cuentas de correo, dominios y direcciones IP.
- Capacidad para soportar la revisión de firmas DKIM en los encabezados de correos entrantes.
- Contar con actualizaciones para sus patrones y motores de detección de spam (heurística), phising y código malicioso.
- Capacidades de colaboración con los centros de investigación de amenazas del fabricante, con la finalidad de reportar de manera automática cualquier comportamiento sospechoso relacionado con el tráfico de correo electrónico.
- Capaz de recibir tráfico con conexiones TLS y poder hacer conexiones con otros servidores de TLS.

- Contar con mecanismos que permitan evitar la recepción de correos de notificaciones dirigidas a cuentas de usuarios no válidos o que no existen el dominio destino (correos de rebote o Bounced Mails).
- Bloqueo automático de IP debido a alta cantidad de envío de spam, ataque tipo DHA (Directory Harvest Attack), Bounced Mails o código malicioso, totalmente parametrizable al número de mensajes recibidos en un intervalo de tiempo determinado a discreción.
- 3.6.0.2.33 o Capacidad para Integrar excepciones, tanto en hosts remitentes como en destinatarios, así como para cuentas de usuarios o dominios específicos.
- 3.6.0.2.34 o Permitir la creación de cuarentenas o carpetas de auditoría de correo, la cuarentena debe poder ser almacenada por la solución como mínimo 30 días.

2.1.8 Antimalware

El Licitante del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Componente Habilitador de Análisis de Tráfico (COLECTOR)
  - No deberá ser disruptivo ante ningún servicio informático que la institución brinde, es decir; no deberá bloquear ningún tráfico, no deberá agregar latencia ni deberá operar "en línea", bajo ninguna circunstancia, sobre ningún paquete de red.
  - La recepción y análisis del tráfico de red deberá ser posible única y exclusivamente mediante la lectura y recepción de puertos de monitoreo (port mirror o port span) que envíen la totalidad del tráfico de red a analizar.
  - La recepción y análisis del tráfico de red deberá ser posible sin la necesidad de integración con ningún servicio o infraestructura de la institución, y sin la necesidad de instalar agentes de software en ningún dispositivo a monitorear.
  - Capacidad de detectar y analizar, dentro del tráfico entregado en la red:
  - Amenazas y riesgos de cualquier dispositivo IP independientemente de su plataforma o sistema operativo, que se conecte a la red monitoreada, y que atente contra la integridad, disponibilidad y confidencialidad del flujo y contenido de la información.
  - Ataques dirigidos con el objetivo de extraer, robar u obtener por medios digitales información.
- Brindar todos los elementos de inteligencia de amenazas necesarios para poder determinar el origen, las acciones y el impacto de la misma con el objetivo de implementar recomendaciones en la infraestructura analizada para poder responder al ataque antes de que cause un daño significativo.
- Capacidad para descubrir el comportamiento malicioso de dispositivos que no cumplen con los requerimientos mínimos de seguridad institucionales.
- Capacidad para poder identificar amenazas que son evasivas a la seguridad tradicional de firewalls, detectores de intrusos y antivirus.
- Brindar un análisis forense de las amenazas en un ambiente de simulación (sandbox) local, automatizado, aislado y personalizado con base a la infraestructura y configuración específica, tanto de sistema operativo como de aplicaciones instaladas en los equipos.
- El ambiente de simulación deberá soportar sistemas operativos simulados de la plataforma Windows 7, 8.x , server 2003 y 2008, en sus versiones de 32 y 64 bits, o su ultima versión liberada por el fabricante.
- Capacidad para poder identificar amenazas utilizando inteligencia global, inteligencia local, inteligencia personalizada y correlación entre las mismas.

- Capacidad para correlacionar información de protocolos y sesiones en todo el volumen del tráfico analizado, identificando posibles riesgos y amenazas de seguridad.
- Detectar y correlacionar comportamientos del atacante en la red interna como por ejemplo:
  - Movimiento lateral
  - Accesos y consultas a bases de datos
  - Transferencia de archivos
  - Accesos a escritorios remotos
- Capacidad para poder obtener el usuario de directorio activo involucrado en el incidente aun cuando el dominio no sea el institucional sin la necesidad de integración directa con el directorio activo de la institución.
- Capacidad para poder analizar no sólo archivos ejecutables, sino también archivos de documentos que puedan ser utilizados para explotar vulnerabilidades en aplicaciones independientes al sistema operativo.
- Capaz de detectar servicios DNS, DHCP y SMTP no declarados a la institución.
- Capaz de detectar aplicaciones móviles maliciosas.
- Capaz de detectar dispositivos móviles accediendo a servidores críticos, a través de escritorio remoto (protocolo RDP).
- Capaz de identificar y analizar amenazas transmitidas en al menos 80 protocolos de red, en cualquier puerto, tanto tráfico entrante como saliente, incluyendo HTTP, SMTP, POP3, FTP, DNS, IRC, SMB, RDP, SQL, IMAP4 y Bittorent, entre otros.
- Capacidad para brindar la información disponible, en todo momento, de los incidentes de seguridad detectados a través de un tablero de resultados (dashboard).
- Capacidad para poder detectar mecanismos de ocultamiento y evasión de análisis de tráfico, redes TOR, UltraSurf, características de tráfico SSL malicioso, entre otras.
- El componente habilitador deberá poder notificar de sus hallazgos utilizando los siguientes formatos, CEF, LEEF, Syslog, SNMP o SMTP.
- De ser requerido, el componente habilitador podrá instalarse dentro de un ambiente virtual (VmWare, Hyper-V, KVM, entre otras) para analizar tráfico dentro de la infraestructura virtual de la institución utilizando el virtual Switch.
- Capacidad de configurar inteligencia local personalizada que permita la detección de los siguientes componentes:
  - Archivos mediante SHA-1 o SHA-2 ingresado manualmente o mediante la subida de un archivo
  - Direcciones IP
  - URL
  - Dominios
- Componente Habilitador de Retroalimentación y Respuesta Automática (ANALIZADOR)
  - Capacidad para proveer inteligencia y contramedidas a la infraestructura existente de seguridad para correo externo, correo interno, web, servidores y puestos de servicios.
  - Capacidad para poder recibir, analizar y diagnosticar de manera automática, archivos adjuntos, y documentos PDF, Word, Excel, ZIP, Flash, entre otros, que provengan de las soluciones de seguridad de correo externo, correo interno y web.
  - Capacidad para poder recibir muestras externas, archivos, URLs o listas de URLs, para su análisis, alimentadas de la siguiente forma, entre otras:
    - Alimentación manual mediante consola Web
    - Utilizando APIs y WebServices
    - Alimentación automática proveniente de la infraestructura existente mediante la utilización de repositorios

2.1.9 Firewall Especializado en Servicios Web (WAF)

El Licitante del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Inspección y análisis de perfiles de comportamiento normal de usuarios para detectar y mitigar el uso anormal de aplicativos Web.
- Soportar un throughput de 10 Gbps en capa 7.
- Soportar 100,000 Transacciones por Segundo (TPS)
- Servicio de reputación para identificar/bloquear ataques automatizados y/o usuarios maliciosos.
- Detección de ataques por clientes automatizados y robots.
- Detección de URL rewriting u ofuscación del URL.
- Capacidad para soportar inspección del protocolo XML.
- Certificado por organismos de la industria como ICSA Labs o PCI.
- Actualización automática de firmas de prevención contra código malicioso.
- Protección contra ataques/vulnerabilidades conocidas (OWASP), de manera enunciativa más no limitativa:
    - SQL injection
    - Cross Site Scripting
    - Cross Site Request Forgery
    - Sensitive Data Exposure
    - Security Misconfiguration
    - Broken Authentication and Session Management
    - Otras nuevas identificadas por OWASP
- Soportar formatos de mensaje: Web 2.0, HTML, XHML, HTML5, XML, JSON, AJAX, FLASH, JavaScript, de manera enunciativa mas no limitativa.
- Soportar Protocolos: TCP,HTTP,HTTPS,SSL/TLS
- Soportar Mitigación de manera enunciativa mas no limitativa al menos las siguientes amenazas:
    - HTML Content Aware
    - Intrusion Detection and Prevention (URI patterns)
    - URI rate-based heuristics
    - Vendor Vulnerabilities
    - URL cloaking / rewrite
    - Parameter Inspection
    - Learning mode

2.1.10 Firewall especializado en Base de Datos

El Licitante del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Tecnología de auto-aprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo schemas, objetos, tablas; sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario.
- Deberá operar a nivel local y en la capa de red
- Deberá soportar al menos los siguientes motores de Bases de Datos:
    - Microsoft SQL Server

  - Oracle
  - Sybase
  - Informix
  - MySQL
  - Progress
  - PostgreSQL
- Proporcionar protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.
- En caso de ser necesario la utilización de agentes, estos deberán soportar al menos los siguientes Sistemas Operativos:
  - AIX
  - HP-UX
  - Solaris
  - RHEL
  - SusE
  - OEL
  - Windows 32/64 bits
- Capacidad para funcionar independiente a la activación de la auditoría nativa de la base de datos.
- Transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
- Se requiere un repositorio para el registro de la actividad, el cual no deberá ser accesible por ningún otro mecanismo que no sea la interacción mediante la GUI (interfaz gráfica) proporcionada por el fabricante o por medios administrativos debidamente asegurados.
- Capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de comunicación, y configuración de seguridad, sin importar el sistema operativo sobre el que se encuentren instaladas.
- Capacidad para poder realizar descubrimientos automatizados en la red para identificar nuevas bases de datos siendo habilitadas, ya sea a nivel de servidor o puertos habilitados en servidores conocidos.
- Capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo a las políticas de negocio. Las definiciones de tipo de dato deberán poder crearse de manera flexible y granular.
- Capacidad para proveer un servicio de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.
- Deberá apoyar en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y Control de cambios.
- Deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
- Deberá monitorear e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, ligas, stored procedures, entre otros.
- Deberá hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.

- Capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.
- Capacidad para proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.
- Deberá manejar reglas y políticas tan amplias o granulares como se requieran y deberán poder ser construidas automáticamente o manualmente y deberán poder ser actualizadas, igualmente, de forma manual o automática.
- Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:
    - Número de registros a regresar por la consulta (SQL Query)
    - Número de registros afectados
    - Tipo de datos accesado (financiero, recursos humanos, inventarios, o cualquier definición personalizada)
    - Acceso a datos marcados como sensibles
    - Base de Datos, Schema, Instancia, Tabla y Columna accesada
    - Estado de autenticación de la sesión
    - Usuario y/o Grupo de Usuarios de Base de Datos conectado
    - Usuario conectado en la capa aplicativa, a diferencia del usuario conectado a la DB
    - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier customización por expresiones regulares)
    - Logins, Logouts, Queries
    - IPs de origen y destino
    - Nombre de Host origen, Usuario firmado en el Host origen
    - Aplicación usada para la conexión a la base de datos
    - Tiempo de respuesta/procesamiento del query
    - Errores en el manejador de SQL
    - Número de ocurrencias en intervalos de tiempo definidos
    - Por operaciones básicas (Select, Insert, Update, Delete)
    - Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export)
    - Por Stored Procedure o Function utilizada
    - Si existe ticket asignado de cambios
    - Hora del Día
- Deberá posibilitar los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.
- Deberá proteger contra ataques SQL y no-SQL.
- Contar con un mecanismo de actualización de la inteligencia interna de seguridad, que incluye las pruebas de las evaluaciones de vulnerabilidad, las firmas contra ataques, la granularidad de las políticas de seguridad y defensas contra comportamientos conocidos.
- Considerar de emergencia, para potenciales violaciones de la información que incluyan, enunciativa más no limitativamente:
    - Altos volúmenes de acceso a datos sensibles más allá de lo habitual.
    - Acceso a datos inusual para cierta hora del día.
    - Acceso a datos desde una ubicación (física) desconocida.
    - Acceso a datos utilizando aplicaciones/herramientas no autorizadas.
- Debe manejar una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.

ANEXOS

DIRECCIÓN DE CONTRATOS

- Debe tener facilidades de Archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP)
- Deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.
- Deberá contar con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de las mismas.
- Deberá soportar y aplicar simultáneamente un modelo de seguridad positivo y negativo.
- El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que deberá además cumplir con las siguientes especificaciones:
  - Deberá bloquear las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
  - Deberá incluir una lista pre-configurada y detallada de las firmas de ataque.
  - Deberá permitir la modificación o adición de firmas por el administrador.
  - Deberá permitir la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
  - Deberá detectar ataques conocidos a nivel base de datos.

2.1.11 Centro de Operaciones de Seguridad (SOC)

Perfil	Certificaciones a demostrar	Función	Número de recursos
Administrador del Centro de Operaciones de Seguridad (SOC en sitio y remoto)	CISM (Certified Information Security Manager)	Responsable de la administración, monitoreo, operación de los servicios proporcionados por el SOC, así como del soporte, atención a fallas e incidentes de seguridad.	1 recurso
Administración y Operación de controles tecnológicos	Consultor especializado en cada una de las soluciones de seguridad integradas. Se aceptan como documentos comprobables el certificado vigente o constancias de los cursos de capacitación que haya tomado directamente del fabricante.	Operar administrar y monitorear las soluciones de seguridad propuestas.	Al menos 3 recursos
Analista de Seguridad	CEH (Certified Ethical Hacker)	Encargado de ejecutar las revisiones de seguridad sobre	Al menos 1

Perfil	Certificaciones a demostrar	Función	Número de recursos
		las aplicaciones y la infraestructura, así como prever, detectar, analizar, contener, erradicar, documentar incidente de seguridad.	
Líder de proyecto	PMP (Project Manager Professional) Certificado por PMI o ITIL v3 (Expert o Master)	Es la persona encargada de administrar y coordinar el proyecto.	Al menos 1
Operador de la mesa de servicio SOC	ITIL v3 Foundation Certification	Personal encargado de las operaciones de soporte de primer nivel, el monitoreo de los servicios, así como del registro y seguimiento de solicitudes de ventanas de mantenimiento, reportes de fallas y requerimientos.	Al menos 3, o los necesarios para garantizar el servicio 7x24x365 durante la vigencia del contrato
Consultor de Penetración	GPEN (GIAC Certified Penetration Tester) o CEH (Certified Ethical Hacker) Examiner) o CICP (Core Impact Certified Profesional)	Realizar simulacros de ataque a la red de la infraestructura o las aplicaciones para determinar lo que los atacantes pueden acceder y qué problemas pueden causar. Evaluar la seguridad de la infraestructura de red y aplicaciones utilizando herramientas y técnicas que un atacante podría utilizar	Al menos 1 recurso
Consultor Forense de Cómputo	EnCE (EnCase Certified Examiner) o CHFI (Certified Hacker Forensics Investigator)	Analizar, en el supuesto de un ataque y penetración exitoso a la infraestructura, la metodología de ataque para determinar cómo se logró, cuál fue el alcance del daño, logrando así determinar las medidas preventivas a implementar. Debe tener la capacidad de ejecutar investigaciones forenses en caso de ser necesario.	Al menos 1 recurso

ANEXOS

DIVISIÓN DE CONTRATOS

3. Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Ing. Héctor Javier Reyes Oropeza	Titular de la División de Administración, Procesamiento y Almacenamiento		12/11/2019
Lic. Carlos Francisco Ramirez Del Rivero	Titular de la División de Administración y Continuidad de la Operación		12/11/2019
Mtro. Hector Martinez Valenzuela	Titular de la División de Telecomunicaciones		12/11/2019
Mtro. Alejandro Paniagua Ramirez	Titular de la División de Administración de Riesgos Tecnológicos		12/11/2019

Revisó	Cargo	Firma	Fecha
Ing. Javier Cortés López	Titular de la Coordinación Técnica de Operación de Servicios Tecnológicos		12/11/2019
Ing. Carlos Calderon Zacarias	Titular de la Coordinación Técnica de Redes y Telecomunicaciones		12/11/2019

Aprobó	Cargo	Firma	Fecha
Ing. Eduardo Oropeza Ortíz	Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional		12/11/2019

Servicio de Continuidad de la Nube IMSS 2020

Apéndice #6. Métricas de Niveles de Servicio

Contenido

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	28/10/2019	Elaboración de documento	Ing. Héctor Javier Reyes Oropeza Lic. Carlos Francisco Ramírez del Rivero Ing. Héctor Martínez Valenzuela Ing. Alejandro Paniagua Ramírez
0.2	04/11/2019	Actualización del documento	Ing. Javier Cortés López Ing. Carlos Calderón Zacarías
1.0	12/11/2019	Aprobación del documento	Ing. Eduardo Oropeza Ortiz

ANEXOS
DIVISIÓN DE CONTRATOS

1. Objetivo del documento

El presente Apéndice tiene como fin establecer los objetivos y las métricas de los niveles de servicio para cada uno de los servicios administrados señalados en los apartados de "Descripción de Servicios" y "Niveles de Servicio" del Anexo Técnico, apéndices, términos y condiciones, anexos, oferta del licitante, y documentación contractual.

De igual forma se señalan las penalizaciones y deductivas que aplican en caso de incumplimientos por parte del prestador del servicio.

Las métricas de niveles de servicio consideradas se clasifican como: de Disponibilidad Directa, de Disponibilidad Indirecta y de Entrega del Servicio, donde:

- **Disponibilidad Directa**: Se refiere a la disponibilidad de uso de un BCF con motivo de su propia operación o de sus propios componentes, en cuyo caso, será objeto de deducciones por la prestación deficiente del servicio. Por disponibilidad directa también se deberán incluir a los eventos de gestión de cambios, incidentes, problemas, eventos, configuraciones, fallas y toda aquella acción donde se afecten o degraden servicios no autorizados, sin un CRQ o se efectúen acciones que ocasionen indisponibilidad directa a diversos componentes de infraestructura.

- **Disponibilidad Indirecta**: Se refiere a la indisponibilidad, afectación, degradación de uno o más BCFs con motivo de la indisponibilidad directa de otro BCF del cual dependa para su operación, por lo que, el(los) BCF(s) con indisponibilidad indirecta también será(n) objeto de deductivas al ser afectada su operación. Por ejemplo, tal es el caso de una falla en el servicio del firewall y con ello se afecte la disponibilidad de todos los BCFs que están protegidos por el mismo firewall, con lo que los BCFs a deducir serán todos aquellos con afectación directa y también lo de afectación por indisponibilidad indirecta.

  Es importante mencionar, que el concepto de indisponibilidad directa se aplicará aun y cuando no sea hayan solicitado las agrupaciones de los BCCs por el GCC, ya que si bien no hubieran sido solicitadas las agrupaciones BCC, estas afectaciones indirectas ocasionan afectaciones en la operación de los servicios Institucionales, por lo que se aplicarán siempre sobre todos los BCFs que resulten afectados de manera directa o indirecta sin menoscabo de tener habilitado o no la agrupación BCC.

  Por disponibilidad indirecta también se deberán incluir a los eventos de gestión de cambios donde se afecte la disponibilidad de servicios no autorizados, no exista CRQ o se efectúen acciones que ocasionen indisponibilidad indirecta a diversos componentes de infraestructura y componentes de software, así mismo se deberán incluir todas las afectaciones causadas por reinicios, afectaciones, fallas humanas en la operación o fuera de los planes de trabajo en procesos de gestión de la operación.

- **Entrega del Servicio**: Se refiere a la entrega de elementos de los servicios del presente anexo, por mencionar algunos tales como: Incidentes, Cambios, Configuraciones, Problemas y Solicitudes de la Operación de los Servicios, dentro de los cuales se aceptarán las ventanas de mantenimiento solicitadas y documentadas como necesarias por parte del licitante, hasta el tiempo señalado por la ventana de mantenimiento solicitada,

por lo que en caso de entregas fuera del nivel de servicio establecido, serán motivo de las deductivas y penas convencionales correspondientes.

Dichas métricas aplican de manera general y obligatoria para todos los servicios descritos en el catálogo de servicios del Anexo Técnico, sin menoscabo que en algunos casos aplican criterios particulares de acuerdo a las características propias del servicio.

2. Métrica de Disponibilidad

La métrica general para el cálculo de la disponibilidad directa y/o de la disponibilidad indirecta, se medirá según la siguiente fórmula:

$Disponibilidad_i = 100 * (TRO_i / (TTM_i - TPFO_i))$

En donde:

- $Disponibilidad_i$ Se refiere a la disponibilidad de la instancia del bloque de construcción BC_i que puede ser instanciado de un BCF o BCC.
- Se calculará para cada $i = 1...n$, de cada BC_i activo en el mes, donde n es el numero total de instancias activas de dichos BCs.
- Tiempo Real de Operación (TRO_i): Es el tiempo total durante el cual el servicio estuvo disponible durante el periodo evaluado del BC_i.
- Tiempo Total Mensual (TTM_i): Es el tiempo total de operación que tiene el mes respectivo del BC_i.
- Tiempo Planeado Fuera de Operación ($TPFO_i$): Es el tiempo en que el servicio se encuentra fuera de operación debido a mantenimientos planeados y programados de manera anticipada para el BCC_i o BCF_i. Este rubro será un caso eventual pues el mantenimiento deberá ser en horarios fuera de operación.

Notas:

- Todos los tiempos son medidos en minutos enteros redondeados.
- Todas las ventanas de mantenimiento estarán sujetas a la autorización previa del Instituto, en particular de equipo asignado a la Continuidad operativa y gestión de la operación de la Nube IMSS.
- Se debe considerar la disponibilidad de los servicios mensuales en un horario de 7x24x265
- El tiempo de inicio de la indisponibilidad será a partir de la primera notificación que se realice de la indisponibilidad de algún servicio o aplicación afectado por la indisponibilidad de un BC, dicha notificación puede ser por: la herramienta de monitoreo implementada, un reporte de parte del Instituto, un reporte por parte del área usuaria interna o externa al Instituto o bien, cualquier medio por el cual se detecte la indisponibilidad del servicio o aplicación afectado y concluirá una vez que el Instituto efectué la validación de la recuperación del servicio o aplicativo afectado.
- El tiempo de indisponibilidad será acumulable durante el periodo de medición, es decir, se considerará la sumatoria de los lapsos de tiempo fuera de servicio durante el periodo mensual de pago.
- Las deductivas por incumplimiento se aplicarán por cada punto porcentual o fracción debajo del objetivo.

Los niveles de servicio establecidos para la prestación del servicio son los siguientes:

Modalidad	BCF o BCC mensual	
M1	Disponibilidad Directa e Indirecta *	99.982%
M3	Disponibilidad Directa e Indirecta *	99.982%
M5	Disponibilidad Directa e Indirecta *	99.982%
M6	Disponibilidad Directa e Indirecta *	99.982%
Deficiencias en la entrega de documentación	Deficiencias en la calidad, consistencia o congruencia de la información en la entrega de documentación (documentos post mortem, documentos de análisis, reportes, documentos probatorios de la prestación de los servicios adjuntos al proceso de facturación, así como todo tipo de documentación relacionada en el presente anexo técnico) parcial o total.	

** Periodo mensual en porcentaje de disponibilidad*

Dónde:
M1: Centro de Datos externo (Centro de Datos Primario),
M3: Extensión de Nube Privada (ENP) en los puntos con mayor demanda transaccional de operación de los servicios del Instituto,
M5: Instalaciones designadas por el Instituto, y
M6: Ambientes no productivos para el apoyo a la evolución y desarrollo tecnológico

A continuación se presentan las consideraciones generales que aplicarán para el cálculo mensual de la Métrica de Disponibilidad:

1. Nivel de Servicio Objetivo (SLAO): Es el Nivel de Servicio que como mínimo debe cumplirse para cada uno de los servicios descritos en el Anexo Técnico, apéndices, términos y condiciones, anexos, oferta del licitante, y documentación contractual. Su medición es por dispositivo o Configuration Item (CI´s) que en este servicio se denominan BCFs y BCCs en sus modalidades de indisponibilidad directa o indisponibilidad indirecta.
2. Nivel de Servicio (SL): Es el Nivel de Servicio efectivamente entregado por el proveedor o prestador de servicio durante el intervalo de medición correspondiente. En un entorno multicomponente, es el mínimo valor reportado de entre todos los componentes del servicio (BCFs o BCCs según correspondan), por lo que en caso de que los demás componentes estén operativos pero la indisponibilidad indirecta sea por un número reducido de BCFs o

BCCs, aun así, todos los componentes afectados (indisponibilidad indirecta) serán calculados hasta que el componente que los afecta a los restantes se restablezca.

3. Número de servicios afectados (n): Es el número de servicios afectados descritos dentro del alcance del Anexo Técnico apéndice, términos y condiciones, anexos, oferta del licitante, y documentación contractual. El % de Deductiva Bruta = (SLAO - SL). Este valor será aplicable únicamente cuando el valor del porcentaje de la deductiva bruta sea positivo.
4. Deductiva a aplicar al licitante ganador = (n * Monto del servicio correspondiente entregado por el proveedor o prestador de servicio).

3. Penalizaciones y Deducciones al Pago

4.1 Penas Convencionales

Se le aplicará al proveedor una pena convencional por el atraso en el cumplimiento de las fechas pactadas de inicio en la prestación del servicio o cualquier compromiso de entrega derivado de los servicios del presente anexo técnico y los tiempos establecidos para métrica de entrega descrita en el presente apéndice.

Para el caso del inicio del servicio, el 1° de enero del 2020, la pena convencional por atraso en la entrega de la infraestructura necesaria para dar continuidad a los servicios Institucionales, será del 2.5% (dos punto cinco por ciento) por cada día natural de atraso en la entrega respecto al costo anual del servicio ofertado.

Un mes posterior al inicio del servicio, la penalización diaria será de 2.5% (dos punto cinco por ciento), por cada día natural de atraso en la entrega de infraestructura de procesamiento, almacenamiento, respaldos, telecomunicaciones (LAN, WAN, Punto Neutro y cableados), seguridad, licenciamiento (open source o con costo), habilitación de infraestructura virtual, configuraciones así como cualquier elemento en el ecosistemas del Instituto (productivo, no productivo, pruebas, entre otros), respecto al costo mensual del servicio ofertado al cual corresponda el incumplimiento en los niveles de servicio por parte del proveedor, sobre las fechas establecidas de entrega.

Para el caso de documentación y sus tiempos de entrega (documentos post mortem, documentos de análisis, reportes, documentos probatorios de la prestación de los servicios adjuntos al proceso de facturación, así como todo tipo de documentación relacionada en el presente anexo técnico), la penalización diaria será de $2,500.00 pesos 00/100MN (dos mil quinientos pesos 00/100MN) por cada día natural de atraso en la entrega.

La pena convencional se calculará multiplicando el porcentaje de penalización diaria por el número de días de atraso, y el resultado se multiplicará por el valor de los servicios entregados con atraso. La penalización tendrá como objeto resarcir los daños y perjuicios ocasionados al Instituto, con motivo de dichos incumplimientos. En conjunto, la cantidad de la penalización no deberá exceder el monto del porcentaje de la garantía de cumplimiento del contrato.

A continuación se señalan los casos en los que aplicará dicha pena contractual:

1. Por el atraso en el cumplimiento de las fechas pactadas de inicio en la prestación del servicio
2. Por no presentarse a la reunión inicial y mesas de trabajo.

3. Por no presentar los planes de trabajo general y/o detallado en la fecha acordada.
4. Por no presentar cualquiera de los entregables señalados en los servicios del presente anexo técnico, apartado denominado "Descripción de los Servicios" del Anexo Técnico apéndices, términos y condiciones, anexos, oferta del licitante, y documentación contractual. Cada uno de los entregables omitidos se considera un evento independiente sujeto a la penalización correspondiente en el servicio relacionado con dicho entregable.

   Fórmula: (%pd) x (nda) x (vbsepa) = pca

   Dónde:

   %: Porcentaje
   pd: Penalización diaria
   nda: Número de días de atraso
   vbsepa: Valor de los servicios entregados con atraso
   pca: Pena convencional aplicable

4.2 Deducciones por Incumplimiento de Niveles de Servicio (SLAs)

A continuación se presentan las tablas que relacionan las deductivas por incumplimiento a los objetivos de las métricas de Niveles de Servicio relacionadas con los servicios administrados de Nube IMSS descritos en el apartado de "Descripción de Servicios" del Anexo Técnico.

4.2.1 Deductivas sobre SLAs aplicables a todos los servicios del Anexo Técnico

Modalidad	BCF o BCC mensual	
M1	Disponibilidad Directa e Indirecta *	99.982%
	Deducción**por cada centésima porcentual (0.01%) o fracción fuera del nivel de servicio	2%
M3	Disponibilidad Directa e Indirecta *	99.982%
	Deducción**por cada centésima porcentual (0.01%) o fracción fuera del nivel de servicio	1%
M5	Disponibilidad Directa e Indirecta *	99.982%
	Deducción**por cada centésima porcentual (0.01%) o fracción fuera del nivel de servicio	1%
M6	Disponibilidad Directa e Indirecta *	99.982%
	Deducción**por cada centésima porcentual (0.01%) o fracción fuera del nivel de servicio	1%
Deficiencias en la entrega de documentación	Deficiencias en la calidad, consistencia o congruencia de la información en la entrega de documentación (documentos post mortem, documentos de análisis, reportes, documentos probatorios de la prestación de los servicios adjuntos al proceso de facturación, así como todo tipo de documentación relacionada en el presente anexo técnico) parcial o total.	-

	Deducción por cada día natural posterior a la fecha establecida de entrega, en la que cada documento presentado por el proveedor continúa con deficiencias en la calidad.	$1,000.00 00/100 MN

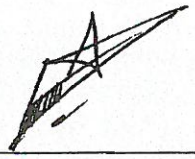
* Periodo mensual en porcentaje de disponibilidad
**Deducciones por incumplimiento sobre el precio unitario mensual del BCF o BCC afectado Por cada centésimo porcentual (0.01%) o fracción de disponibilidad fuera del nivel de servicio solicitado

Dónde:
M1: Centro de Datos externo (Centro de Datos Primario),
M3: Extensión de Nube Privada (ENP) en los puntos con mayor demanda transaccional de operación de los servicios del Instituto,
M5: Instalaciones designadas por el Instituto, y
M6: Ambientes no productivos para el apoyo a la evolución y desarrollo tecnológico

4. Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Ing. Héctor Javier Reyes Oropeza	Titular de la División de Administración, Procesamiento y Almacenamiento		12/11/2019
Lic. Carlos Francisco Ramirez Del Rivero	Titular de la División de Administración y Continuidad de la Operación		12/11/2019
Mtro. Hector Martinez Valenzuela	Titular de la División de Telecomunicaciones		12/11/2019
Mtro. Alejandro Paniagua Ramirez	Titular de la División de Administración de Riesgos Tecnológicos		12/11/2019

ANEXOS
DIVISIÓN DE CONTRATOS

Revisó	Cargo	Firma	Fecha
Ing. Javier Cortés López	Titular de la Coordinación Técnica de Operación de Servicios Tecnológicos		12/11/2019
Ing. Carlos Calderon Zacarias	Titular de la Coordinación Técnica de Redes y Telecomunicaciones		12/11/2019

Aprobó	Cargo	Firma	Fecha
Ing. Eduardo Oropeza Ortíz	Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional		12/11/2019

Servicios de Continuidad de la Nube IMSS 2020

Apéndice #7. Glosario Nube IMSS

Contenido

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	14/10/2019	Elaboración de documento	Ing. Héctor Javier Reyes Oropeza Lic. Carlos Francisco Ramírez del Rivero Ing. Héctor Martínez Valenzuela Ing. Alejandro Paniagua Ramírez
0.2	28/10/2019	Actualización del documento	Ing. Javier Cortés López Ing. Carlos Calderón Zacarías
1.0	12/11/2019	Aprobación del documento	Ing. Eduardo Oropeza Ortiz

ANEXOS

DIVISIÓN DE CONTRATOS

1. Objetivo del documento

El objetivo del presente Apéndice es definir conceptos y acrónimos que se utilizan en el anexo técnico objeto de la presente Licitación.

2. Glosario

Acuerdo de Nivel Operacional (OLA). Documento interno de la organización donde se especifican las responsabilidades y compromisos de los diferentes departamentos de la organización TI en la prestación de un determinado servicio. En la organización de TI puede haber áreas del Instituto y proveedores de servicios tecnológicos.

Acuerdo de Nivel de Servicio (SLA). Un acuerdo entre un proveedor de Servicios de TI y el Instituto. Describe el Servicio de TI, documenta las metas de niveles de servicio y especifica las responsabilidades del proveedor de Servicios de TI y del Instituto.

Alerta. Notificación que un umbral ha sido alcanzado, que algún componente ha cambiado o un error a ocurrido.

Alta Disponibilidad. Táctica para minimizar u oculta los efectos del fallo de algún elemento de configuración con la finalidad de garantizar el cumplimiento de la disponibilidad de un servicio.
Ambiente. Un subconjunto de la Infraestructura de TI que se usa con un propósito particular. Por ejemplo Producción, Desarrollo, Pruebas, etc.

Arquitectura. La organización fundamental de un sistema representada por sus componentes, sus relaciones entre ellos y con su entorno, y los principios que gobiernan su diseño y evolución

Backup o Respaldo. Copia de los datos a fin de protegerlos contra una pérdida de Integridad o de Disponibilidad del original.

Base de Datos de Errores Conocidos. Una base de datos que contiene todos los registros de errores conocidos.

Biblioteca Definitiva de Medios. Una o más ubicaciones en las que las versiones definitivas y aprobadas de todos los Elementos de Configuración de servicios se almacenan de modo seguro.

Servicio de caché. Servicio distribuido que almacena contenido en memoria a fin de mejorar el desempeño en la entrega de contenidos Web a través del Internet.

Cambio. La adición, modificación o la eliminación de cualquier elemento que afecte a los Servicios de TI.

Cambio Emergente. Un cambio que se debe de implementar cuanto antes.

Cambio Normal. Un cambio preaprobado que implica un riesgo bajo que sigue un procedimiento y un plan de trabajo.

Canales digitales. Se refiere a la posibilidad de gestionar diferentes canales; "enrutar" los mensajes en función de quien los emite explicitando el motivo; gestionar alarmas y acciones que permitan anticiparse y ser proactivos en el servicio al cliente; obtener y medir los KPIs correctos para esta gestión.

Capacidad. El rendimiento máximo que un Elemento de Configuración o un Servicio de TI puede presentar sin dejar de cumplir los Niveles de Servicio acordados.

Causa Raíz. La causa origen de un Incidente o Problema.

Concurrencia. Medida del número de usuarios comprometidos en la misma operación al mismo tiempo.

Confiabilidad. Medida del tiempo en que un Servicio de TI puede realizar su función acordada sin interrupción.

Consejo Consultor de Cambios (CAB). Grupo de personas que cumplen la función de establecer las prioridades y la definición de un calendario de cambios, formado por representantes de la DIDT del Instituto.

Despliegue. Instalación o implantación de un Activo o Servicio de TI dentro de un determinado entorno operativo.

Disponibilidad. Capacidad de un Elemento de Configuración o de un Servicio de TI de ejecutar su función acordada cuando sea requerido.

Dominio Tecnológico: Las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo.

Escalabilidad. La habilidad de un Servicio de TI o un Elemento de Configuración para realizar la función acordada al cambiar la carga de trabajo o el alcance.

Evento. Cambio de estado de un elemento de configuración o Servicio de TI, generalmente puede ser una alerta o una notificación.

Gestión de Incidentes. El proceso encargado del control del ciclo de vida de todos los incidentes.

Gestión de Problemas. El proceso encargado del control del ciclo de vida de todos los problemas.
Impacto. Medida de la afectación que causa un Incidente, Problema o Cambio sobre un Servicio de TI.

Incidente. Interrupción no planeada o una reducción de la calidad de un servicio de TI.
MAAGTICSI. Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información.

Marco de Trabajo de Arquitectura. Es un conjunto de herramientas que puede ser utilizado para desarrollar un amplio espectro de diversas arquitecturas, describiendo una metodología para la definición de un sistema de información en términos de un conjunto de bloques de construcción

que encajen entre sí adecuadamente, proveyendo un vocabulario común y un conjunto de estándares recomendados.

Mesa de Servicio Institucional. Punto único de contacto entre el Proveedor y el Instituto.

Medición. Acción y efecto de medir, de comparar una cantidad con su respectiva unidad, con el fin de averiguar cuántas veces la segunda está contenida en la primera.

Métricas. Criterio de medición.

Middleware. Software de intermediación que permite la comunicación con otros servicios, sistemas o aplicaciones dentro de la Nube Privada.

Monitoreo. Observación repetida de un Elemento de Configuración, Servicio de TI o Proceso con la finalidad de detectar eventos.

Plan de Implementación. Conjunto de actividades relacionadas para desarrollar un producto y probar que se cumpla con los criterios de calidad. Implican cuantificación de esfuerzos, recursos humanos y tiempo, así como el control de riesgos.

Plataforma. Agrupación de infraestructura de hardware, software y recursos humanos destinados a ofrecer recursos tecnológicos diferenciados para implementar servicios.

Problema. La causa de uno o más Incidentes de los que no se conoce la causa raíz.

Puntos de Acceso a la Nube Privada. Estación de trabajo sin un propósito adicional al de permitir acceder a los servicios de Nube Privada particularmente al escritorio en la nube.

Restaurar. Medidas tomadas para que un Servicio de TI vuelva a su operación normal.

Rezago Tecnológico. Falta de componentes tecnológico o componentes de software o hardware que han dejado de tener soporte por sus fabricantes o que no permiten la integración con estándares vigentes.

Servicio de Aplicación. Un servicio de aplicación se define como un mecanismo para exponer un comportamiento automatizado. Este permite exponer la funcionalidad de los componentes de aplicación a su entorno. Dicha funcionalidad es accedida a través de una o más interfaces de aplicación. El servicio de aplicación debe ser significativo desde el punto de vista del entorno, debe proporcionar una unidad de funcionalidad que es, por sí sola, útil para sus usuarios.

Servicio Digital. Se entiende por servicio digital "a todo servicio que se pone a disposición del usuario a través del Internet o de cualquier adaptación o aplicación de los protocolos, plataformas o de la tecnología utilizada por Internet o cualquier otra red a través de la cual se presten servicios equivalentes mediante accesos en línea y que se caracteriza por ser esencialmente automático y no ser viable en ausencia de la tecnología de la información.

Servicio de Información. Tipo de servicio que proporciona una manera unificada para representar, acceder, mantener, gestionar, analizar e integrar los datos y contenidos desde fuentes de datos heterogéneas

Sistema computacional. Conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

Sistema de Información. Aquellos servicios que habilitan la generación, adquisición, almacenamiento, transformación, procesamiento, recuperación, utilización, análisis o entrega de información, e incluyen los servicios que definen las entidades de negocio, servicios de consulta de información, procesos internos de soporte (backoffice) y servicios de inteligencia de negocio y analítica.

Solicitud de Cambio. Solicitud para que se realice un cambio.

TOGAF. Marco de trabajo de Arquitectura Empresarial (del inglés, The Open Group Architecture Framework).

Petición de Trabajo de Arquitectura. Es un documento que envía el grupo de gobierno de los servicios de arquitectura, gobierno y gestión del conocimiento a la organización de arquitectura para describir (en un alto nivel) las necesidades del Instituto (Objetivos, Interesados, planes estratégicos, etc.)

Declaración de Trabajo de Arquitectura. Es un documento que da respuesta a la Petición de Trabajo de Arquitectura, el cual describe un plan de trabajo general en el que se propone como las soluciones a los problemas que se han identificado, serán abordadas a través del proceso de Diseño de Arquitectura Institucional.

Proceso de Negocio Automatizado. Se refiere al conjunto de funciones o actividades de un proceso de negocio que han sido automatizadas o semiautomatizadas a través de Servicios de Aplicación o el uso de tecnologías de la información.

Tarjeta Inteligente. Una tarjeta inteligente (smart card) es una tarjeta del tamaño del bolsillo con circuitos integrados, que permite la ejecución de cierta lógica programada. Aunque existe un diverso rango de aplicaciones, hay dos categorías principales. Las tarjetas de memoria contienen sólo componentes de memoria no volátil y posiblemente alguna lógica de seguridad. Las tarjetas microprocesadoras contienen memoria y microprocesadores.

3. Tabla de Acrónimos

Acrónimo	Descripción
IMSS	Instituto Mexicano del Seguro Social
DIDT	Dirección de Innovación y Desarrollo Tecnológico
PND	Plan Nacional de Desarrollo
MAAGTICSI	Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información
OLA	Acuerdos de Nivel de Operación (del inglés, Operational Level Agreement)
BCF	Bloques de Construcción Fundamentales
BCC	Bloques de Construcción Comunes
DRP	Plan de Recuperación en caso de Desastres (del Inglés, Disaster Recovery Plan)

ENP	Extensión de Nube Privada
ENH	Extensión de Nube Híbrida
SLA	Acuerdos de niveles de servicios (del inglés, Service Level Agreement)
PDA	Asistente Digital Personal (del inglés, Personal Digital Assistant)
ITIL	Biblioteca de Infraestructura de Tecnologías de Información (del inglés, Information Technology Infrastructure Library)
TIC	Tecnologías de Información y Comunicaciones
SCO	Servicio de Continuidad Operativa
RPO	Punto Objetivo de Recuperación, por sus siglas en inglés
RTO	Tiempo Objetivo de Recuperación, por sus siglas en inglés
VRF	Virtual Routing and Forwarding por sus siglas en inglés
Gbps	Gigabits por Segundo
Mbps	Megabits por Segundo
MB	Megabytes
GB	Gigabytes
TB	Terabytes
NIST	National Institute of Standards and Technology
IaaS	Infraestructura como un Servicio (del inglés, Infrastructure as a Service)
PaaS	Plataforma como un Servicio (del inglés, Platform as a Service)
SaaS	Software como un Servicio (del inglés, Software as a Service)
BB	Bloque de Construcción (del inglés, Building Block)
CMDB	Base de Datos de Elementos de Configuración (del inglés, Configuration Items Database)
PEP	Portafolio Estratégico de Proyectos
ISP	Proveedor de Servicios de Internet (del inglés, Internet Service Provider)
MPLS	Conmutación Multi-Protocolo mediante Etiquetas (del inglés, Multiprotocol Label Switching)
MOSNI	Marco Operativo de los Servicios de Nube IMSS
MTR	Marco Tecnológico de Referencia
RFI	Solicitud de información (del inglés, Request for information)
CAT	Centro de Arquitectura Tecnológica
CCTV	Circuito Cerrado de Televisión
LED	Diodo Emisor de Luz (del inglés, Light Emisor Diode)
LAN	Red de Área Local (del inglés, Local Area Network)
PAN	Puntos de Acceso a la Nube
EN	Escritorios en la Nube
UANP	Usuario de Acceso a la Nube Privada
ACL	Lista de Control de Acceso (del inglés, Access Control List)
ISO	Organización Internacional para la Estandarización (del inglés, International Organization for Standardization)
API	Interfaz de programación de aplicaciones (del inglés, Application Programming Interface)
RFC	Solicitud de Cambio (del inglés, Request for Change)
CAB	Consejo Consultor de Cambios (del inglés, Change Advisory Board)
ECAB	Consejo Consultor de Cambios Emergentes (del inglés, Emergency Change Advisory Board)

4. Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Ing. Héctor Javier Reyes Oropeza	Titular de la División de Administración, Procesamiento y Almacenamiento		12/11/2019
Lic. Carlos Francisco Ramirez Del Rivero	Titular de la División de Administración y Continuidad de la Operación		12/11/2019
Mtro. Hector Martinez Valenzuela	Titular de la División de Telecomunicaciones		12/11/2019
Mtro. Alejandro Paniagua Ramirez	Titular de la División de Administración de Riesgos Tecnológicos		12/11/2019

Revisó	Cargo	Firma	Fecha
Ing. Javier Cortés López	Titular de la Coordinación Técnica de Operación de Servicios Tecnológicos		12/11/2019
Ing. Carlos Calderon Zacarias	Titular de la Coordinación Técnica de Redes y Telecomunicaciones		12/11/2019

Aprobó	Cargo	Firma	Fecha
Ing. Eduardo Oropeza Ortiz	Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional		12/11/2019

ANEXOS

DIVISIÓN DE CONTRATOS

SIN TEXTO

0163

Contenido

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	14/10/2019	Elaboración de documento	Ing. Héctor Javier Reyes Oropeza Lic. Carlos Francisco Ramírez del Rivero Ing. Héctor Martínez Valenzuela Ing. Alejandro Paniagua Ramírez
0.2	28/10/2019	Actualización del documento	Ing. Javier Cortés López Ing. Carlos Calderón Zacarías
1.0	12/11/2019	Aprobación del documento	Ing. Eduardo Oropeza Ortiz

0164

ANEXOS

DIVISIÓN DE CONTRATOS

1. Objetivo del documento

Definir al **LICITANTE** los términos y condiciones del **Servicio de Continuidad de la Nube IMSS 2020**.

2. Alcance del Servicio

Brindar continuidad operativa de los servicios que permiten al Instituto disponer de las capacidades de procesamiento, almacenamiento, respaldo, comunicaciones, seguridad, plataformas tecnológicas y software bajo las **modalidades de despliegue** siguientes:

- **M1**: Centro de Datos externo (Centro de Datos Primario),
- **M3**: Extensión de Nube Privada (ENP) en los puntos con mayor demanda transaccional de operación de los servicios del Instituto,
- **M5**: Instalaciones designadas por el Instituto, y
- **M6**: Ambientes no productivos para el apoyo a la evolución y desarrollo tecnológico

Estos servicios serán consumidos en tres modalidades:

- Los servicios relacionados a lo que se define como "**Nube Privada**", soportan entre otros, sistemas transaccionales del Instituto, aplicativos y tecnologías para servicios digitales y de información, bases de datos, medios de almacenamiento, software de productividad, y en general, aquellas tecnologías que están definidas expresamente para utilización del personal o para otorgar al público un servicio del IMSS bajo control del mismo. Estos servicios deberán extenderse en las modalidades de despliegue de: Centro de Datos externo (Primario) y en Nodos de Extensión de la Nube Privada que se desplegarán conforme a lo indicado de manera referencial en el apéndice "Ubicaciones Geográficas".

- Los servicios relacionados a lo que se define como "**Nube Híbrida**", soportan los servicios aplicativos, digitales y de información, que requieren la interconexión con nubes públicas, privadas y comunitarias. Estos servicios contarán con la capacidad de intercambio de tráfico entre redes de telecomunicaciones, despliegue de canales digitales con reglas específicas de comunicaciones y seguridad, así como la capacidad de extensión de la nube híbrida en regiones geográficas estratégicas para mejorar la experiencia a usuarios externos en la entrega de servicios.

- Los servicios que se definen como de "**Integración a la Nube Privada**", se refieren a la capacidad de consumo tecnológico en las instalaciones designadas por el Instituto, con la finalidad de lograr algún nivel de integración, desde la capacidad de ser accedida a nivel telecomunicaciones, hasta poder consumir o entregar información desde o hacia la Nube Privada.

Los diferentes servicios incluidos dentro de los servicios dentro del presente Anexo Técnico, serán diferenciados tanto por la modalidad de despliegue como la modalidad de Nube. La modalidad de despliegue de Ambientes no productivo, aplicará a las tres modalidades de nube: Privada, Híbrida y de Integración a la Nube Privada.
Los servicios serán medidos a través de acuerdos de Niveles de Servicio, para buscar un uso eficiente y eficaz de los servicios y soluciones, apego a procesos determinados por la normatividad del Instituto, así como el suministro de hardware y software para soporte de las aplicaciones del Instituto, lo que permitirá:

- Flexibilizar y agilizar la atención gradual de requerimientos de infraestructura tanto física como virtual.
- Mantener niveles de operación y de seguridad para la Institución.

- Continuidad en la operación de los servicios digitales y de información, así como de los sistemas informáticos del Instituto.
- Contar con alojamiento de las capacidades de infraestructura y almacenamiento.
- Establecer una estrategia en materia tecnológica para el procesamiento y almacenamiento de información del Instituto, así como el de las plataformas que soportan servicios digitales y de información.
- Monitorear el desempeño de los recursos, dar visibilidad de la disponibilidad de servicios digitales y de información, así como la ejecución de actividades de aprovisionamiento y mantenimiento de infraestructura y plataformas con base en Acuerdos de Nivel de Servicio (SLA's).
- Mantener un esquema de atención a derechohabientes, patrones, proveedores, terceros relacionados y/o público en general que ocupe las diversas aplicaciones, servicios digitales y de información que el Instituto ofrece a través de los diversos canales de atención del Instituto, incluyendo portal de Internet (www.imss.gob.mx), conexiones con terceros, ventanilla, notificaciones y canal móvil, así como contribuir a la transformación digital del Instituto y la atención que presta a sus derechohabientes y patrones.

3. Requerimientos Técnicos

El **LICITANTE** deberá realizar las actividades correspondientes para soportar y operar la infraestructura, aplicaciones y servicios en cualquiera de las modalidades descritas en el presente anexo técnico, garantizando los niveles de servicio señalados en el apartado "Niveles de Servicio" a fin de brindar continuidad a los procesos de negocio internos y externos al IMSS.

El alcance de los servicios descritos en este Anexo Técnico comprende los siguientes elementos, conforme a los servicios descritos en el presente anexo técnico:

- Continuidad operativa y aprovisionamiento bajo demanda de los Bloques de Construcción Fundamentales (BCF) conforme se especifica en el Apéndice "Bloques de Construcción Fundamentales" correspondiente, de acuerdo a cada solicitud específica del Instituto.
- Aprovisionamiento bajo demanda de los Bloques de Construcción Comunes (BCC), partiendo de un ejercicio de planeación con el Instituto para determinar las diferentes plataformas que se requieren; y con base en ellas, establecer la definición y habilitación de los BCC a partir de los BCF.
- Monitoreo y vigilancia del funcionamiento y desempeño de los BCF y BCC, así como de los servicios digitales y de información, y los sistemas informáticos y canales digitales que los soportan y se determinen por el Instituto.
- Continuidad Operativa de la interconexión entre múltiples redes privadas de telecomunicaciones a través de un Punto Neutro de intercambio de tráfico, así como el despliegue de canales de acceso con otras nubes tanto públicas como privadas, en la que destaca el acceso a Internet y varias dependencias públicas, mismas que se identifican en el apéndice "Relación actual de la Infraestructura en Centro de Datos".
- Continuidad Operativa y en su caso aprovisionamiento e instalación de cada nodo de extensión de la nube privada, configuración, puesta en marcha, operación, mantenimiento, soporte y administración de Puntos de Acceso a la Nube Privada con capacidad de despliegue del servicio de Escritorio en la nube.
- Provisión de servicios de administración y monitoreo relacionados a los BCF y BCC de la solución.
- Seguridad y autocontenidos

Una vez iniciados los servicios, el **LICITANTE** deberá brindar continuidad operativa a los servicios del presente anexo técnico y dar cumplimiento al Plan de Trabajo Detallado ofertado, al amparo y

cumplimiento del Plan de Trabajo General descrito en el anexo técnico, con el cual en cuyo caso efectuará la migración de elementos dispuestos en el Servicio actual de Centro de Datos. Una vez que los BCF correspondientes a la migración se encuentren activos y operando en el Centro de Datos ofertado a entera satisfacción del Instituto, podrán ser incorporados al esquema de contraprestación de pagos mensuales.

En apego al mismo Plan de Trabajo General, el licitante deberá presentar en su propuesta un programa de trabajo anual para cada uno de los siguientes servicios:

- Servicio de Continuidad y Gestión de la Operación
- Servicio de Operación y Calidad de la Seguridad informática perimetral
- Servicio de integralidad de ambientes distribuidos a nivel nacional y telecomunicaciones
- Servicio de Gestión de Medición del Desempeño de Aplicativos y Componentes Institucionales

Una vez ofertados y detallados por el licitante estos planes de trabajo en su oferta, y en su caso revisados, modificados, detallados y finalmente aceptados por el Instituto en las reuniones de inicio del contrato, el licitante deberá comenzar a realizar las actividades de habilitación, implementación, puesta punto, operación y administración de cada servicio.

4. Plazo de los servicios

La vigencia del contrato y el plazo para la para la prestación del servicio será a partir del día hábil siguiente del acto de notificación de fallo y hasta el 31 de diciembre de 2020.

La definición de la programación, implementación y desarrollo de los servicios se establece en el correspondiente Anexo Técnico.

ANEXOS
DIVISIÓN DE CONTRATOS

5. Perfil del proveedor

El **LICITANTE** deberá acreditar ser una empresa con la capacidad y experiencia técnica requerida para proporcionar el servicio solicitado, anexando currículo de la misma.

El **LICITANTE** deberá entregar al Instituto "La Opinión del Cumplimiento de Obligaciones en materia de Seguridad Social" vigente y positiva junto con la factura de cobro respectiva mensual, así como entregar el documento vigente expedido por el SAT en el que se emita la opinión de cumplimiento de las obligaciones fiscales, positivo y vigente.

El **LICITANTE** deberá contar con experiencia comprobable para brindar el servicio **"Servicio de Continuidad de la Nube IMSS 2020"** que permitan proveer al instituto la continuidad de los servicios Institucionales que hoy en día operan en el Centro de Datos tercerizado, así como todo el soporte necesario para su funcionamiento, anexando un contrato de las mismas características o similares al que se pretende contratar por parte del IMSS.

El **LICITANTE** deberá contar, con certificaciones en los rubros de procesamiento, comunicaciones, Gestión de Servicios de TI, Administración de Proyectos, Almacenamiento y seguridad, tales como:

- □**CCIE Routing and Switching**
- □**CCIE Service Provider**
- □**CCNP Colaboración**
- □**CCDP Diseño Profesional de redes.**
- □**CCNA Cyber Ops**
- □**ITIL Foundation Certificate in IT Service Management**
- □**ITIL intermediate in Service Design**
- □**ITIL intermediate in Operational support and analysis**
- □**ITIL intermediate in Service Offering AND Agreements**
- □**ITIL intermediate un Release, control and validación.**
- □**Certificación ITIL RCV, 2017**
- □**Certificación ITIL SO, 2016**
- □**Certificación ITIL SOA, 2016**
- □**Certificación ITIL OSA, 2012**
- □**PMI**
- □**Symantec Data Loss Prevention Prevention 14.5**
- □**Symantec Messaging Gateway**
- □**APDS - Avaya Networking Solutions**
- □**APSS - Avaya Networking Solutions**
- □**ISO/IEC 27001**
- □**ISO/IEC 20000**
- □**PCNSE Network Security Engineer 7**
- □**MCITP Enterprise Administrator on Windows Server 2008**
- □**MCTS Microsoft Exchange Server 2007 Configuration**
- □**Extreme Networks Design Specialist - Campus Fabric**
- □**Enterasys Certified Specialist – Routing**
- □**Enterasys Certified Specialist – Policy.**
- □**Security Competency – Technical Accreditation (SCT)**
- □**Network Automation Competency – Technical Accreditation (NCT)**
- □**Core Network Services Competency - Technical Accreditation (CNT)**
- □**CCIE**

El **LICITANTE** debe contar con el personal certificado en Metodologías de Administración de Proyectos para la dirección del proyecto emitido por el Project Manager Institute, cuando menos nivel PMP, presentando la certificación de cuando menos una persona que participará en la prestación del servicio.

El **LICITANTE** deberá presentar al Instituto, a través de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional cita en Av. Paseo de la Reforma No. 476, Anexo de Telecomunicaciones, Planta Alta, Col. Juárez, C.P. 06600, Ciudad de México, en un plazo no mayor a 5 (cinco) días naturales posteriores a la adjudicación del contrato, al personal responsable del proyecto; en caso que no se presente el personal en el plazo marcado, se aplicará la pena correspondiente.

El **LICITANTE** deberá presentar en un plazo no mayor a 10 (diez) días naturales posteriores a la adjudicación del contrato, un plan de trabajo general, para llevar a cabo la implementación del proyecto, en el que se especifiquen las actividades a realizar, la secuencia, los recursos asignados y responsables de dichas actividades, así como la duración del proyecto, su fecha de inicio y de conclusión marcando las fechas de entregables como son cantidad de servicios a entregar de forma única, mensual o eventual.

0166

El **LICITANTE** deberá entregar en un plazo no mayor a 10 (diez) días naturales posteriores a la adjudicación del contrato, una matriz de escalación con el personal que gestionará los servicios de TIC y con los que el Instituto estará colaborando, su cargo y puesto así como los datos y la vía de comunicación para contactarlo.

6. Cumplimiento de obligaciones contractuales

Para la documentación de Cumplimiento de Obligaciones contractuales, el **LICITANTE** elaborará en un plazo no mayor a 10 (diez) días naturales posteriores a la adjudicación del contrato, una matriz de los verbos, pronombres, tiempos y compromisos presentes en el anexo técnico correspondiente, términos y condiciones, apéndices o documentación complementaria al anexo, así como en la propia oferta del **LICITANTE** ganador, a fin de contar con un listado de todos los verbos de acción, conjunciones, excepciones, interacciones, consideraciones de tipo y frecuencia de información electrónica que deba incluirse y en su caso especificaciones o excepciones, para convertirlos en los "documentos probatorios de cada obligación para la prestación del servicio".

A partir de este listado, de manera conjunta entre el **IMSS** y el **LICITANTE**, en un plazo no mayor a 05 (cinco) días naturales posteriores a la entrega del listado por parte del proveedor, generará el detalle de los documentos tanto en formato, contenido, información adjunta en imágenes, archivos o documentos complementarios, así como firmas y validaciones a efectuarse por el personal que participará en los procesos de entrega de servicios, lo cual se depositará en un repositorio documental que habilitará el **LICITANTE** con acceso permanente a los administradores del contrato (cuerpo de gobierno del contrato), los cuales analizarán al menos quincenalmente con el gerente de cuenta y personal técnico por parte del **LICITANTE**, el avance de los proyectos, la continuidad operativa, siguientes compromisos y la documentación del ejercicio del gasto y cumplimiento de niveles de servicio establecidos, siendo parte fundamental la documentación de Cumplimiento de Obligaciones contractuales, incluyendo en su caso, las penas convencionales o deductivas aplicables. En estas juntas de gobierno del contrato, el **LICITANTE** deberá exponer al personal **IMSS**, los detalles de la operación, consumos, tendencias, áreas de oportunidad y mejores prácticas susceptibles de incorporarse a la operación y administración del contrato, las cuales serán evaluadas por el **IMSS** y en su caso, autorizadas con o sin modificaciones, para su implementación y operación gradual o inmediata.

Para la exposición y análisis de la información presentada por el **LICITANTE**, éste deberá habilitar al menos 3 pantallas de al menos 75 pulgadas, con todo lo necesario para la presentación de información de la operación de los servicios tecnológicos que permitan exponer de manera gráfica y ágil lo descrito en los dos párrafos anteriores, así como visualizar la información en línea de la operación de los servicios contratados incluyendo elementos de análisis y detalles de la operación (parámetros de utilización) de la infraestructura ofertada además de la prestación de los servicios, preferentemente reflejando la operación en términos de infraestructura además de indicadores de negocio que puedan ser descritos durante la vigencia del contrato.

7. Clausulas y Cumplimientos

a. Contrato de confidencialidad

El **LICITANTE** entregará al IMSS en un plazo no mayor a 05 días naturales al acto de fallo, una carta de confidencialidad mediante el cual el **LICITANTE** se obliga a no revelar, transferir, compartir ni ceder ningún dato o información de carácter sensible y confidencial que se hayan compartido entre el **LICITANTE** y el **IMSS**.

b. Cláusula de Opción para Obtención de Bienes al cierre de contrato (entregable de infraestructura)

ANEXOS
DIVISIÓN DE CONTRATOS

El último mes de la prestación del servicio, el IMSS podrá evaluar quedarse con los bienes o conservar los bienes para lo cual informará al **LICITANTE** su decisión sobre la opción de compra de los bienes que integran el proyecto, el **LICITANTE** deberá presentar propuesta económica del o los componentes de hardware/software que integran cada uno de los servicios descritos en el presente anexo técnico, así como sujetarse al procedimiento que establezca el IMSS para formalizar este proceso.

Durante el último mes de la prestación del servicio, en caso de que el Instituto haya optado por la opción de compra, el **LICITANTE** realizará el proceso de entrega del equipamiento sujeto a la opción de compra por parte del Instituto. El **LICITANTE** deberá sujetarse al procedimiento que el IMSS requiera para formalizar este proceso.

c. Documentación de cumplimiento de obligaciones

El **LICITANTE** con el objeto de fortalecer la supervisión y vigilancia de la administración del contrato materia del presente servicio y contribuir a las acciones para verificar la procedencia de los pagos, proporcionará un soporte especializado para la gestión del conocimiento administrativo relacionado con la prestación de los servicios de Nube **IMSS**.

Para que dicho conocimiento administrativo sea traducido en un activo del **IMSS**, el **LICITANTE** deberá aplicar el modelo de control de contratos definido por la Coordinación de Sistemas de Infraestructura Tecnológica Institucional (o la correspondiente por funciones organizacionales) y ejecutará las acciones que se establecen en dicho modelo como un ejercicio permanente durante la vigencia del contrato. Para tal efecto, se deberá implementar un mecanismo para que dicho soporte especializado encargado de la gestión del conocimiento administrativo de los servicios objeto del presente anexo, cuente oportunamente con cada una de las solicitudes de servicio que se generen en el marco del contrato respectivo, así como respecto de todos los comunicados y documentos existentes entre el **IMSS** y el **LICITANTE** en relación con la prestación de los servicios. Lo anterior, toda vez que los servicios de soporte especializados previstos en ese aparatado están sujetos a flujo de información antes citada.

Lo anterior, con el fin de que el **LICITANTE** elabore los "Reportes de Administración" con corte mensual, que concluya las acciones relacionadas a la facturación presentada durante el periodo de la prestación del servicio, cuyo contenido se señala a continuación:

Gestión de los servicios: Con base en las solicitudes u órdenes de servicio que genere el **IMSS**, el **LICITANTE** adjudicado incluirá un desglose detallado del trámite que corresponde a la atención de cada una de ellas, en cuanto a su procedencia, tiempos límite de respuestas y demás circunstancias que se encuentren establecidas en el contrato respectivo y que permitan al Administrador del mismo tener control sobre dicha gestión, así como la documentación probatoria del devengo de los servicios, incluyendo toda la documentación o archivos electrónicos que demuestren la prestación del servicio, de conformidad a la funcionalidad solicitada y acorde a los niveles de servicio establecidos, siendo posible entre otros: reportes de monitoreo, disponibilidad, capacidad, desempeño y atención de incidentes, tickets de la mesa, actualizaciones, bitácoras, logs de aplicaciones, entre otros. En caso de que el licitante no cuente con la documentación probatoria de los servicios devengados, estos no podrán ser facturados.

- **Plataforma de obligaciones:** En este apartado, el **LICITANTE** adjudicado elaborará un listado que identifique la totalidad de las obligaciones que se encuentran plasmadas en el

contrato y sus respectivos anexos relacionados con los servicios. Asimismo, llevará a cabo su clasificación en atención a su importancia y consecuencia en:

a. Obligaciones principales. Condicionantes del pago y los que están asociados a penas y deductivas

b. Obligaciones secundarias. No condicionan el pago de los servicios, sin embargo, su cumplimiento es obligatorio en términos del instrumento contractual.

El proveedor deberá presentar la documentación descrita en el presente punto, previo a solicitar el pago de sus servicios.

Asimismo, el **LICITANTE** proporcionará la representación gráfica y analítica de una línea de tiempo en el cual se detallen las fechas límite para el cumplimiento de obligaciones primarias y secundarias conforme a las órdenes de servicio y los plazos y procedimientos previstos en el contrato respectivo.

- **Análisis de consecuencias:** El **LICITANTE** adjudicado realizará un análisis respecto de la aplicación del sistema de sanciones previsto en el contrato durante la vigencia del mismo, con base en las solicitudes u órdenes de servicio recibidas y la atención dada a las mimas. Con esta información el Administrador del Contrato efectuará las acciones de verificación que permitan la aplicación de las reglas de proporcionalidad establecidas en los numerales referentes a penas convencionales y deductivas por prestación deficiente del servicio y su cumplimiento normativo, así como el cálculo de las sanciones que resulten aplicables conforme a lo establecido en el Instrumento Contractual y la normatividad vigente; es este sentido, los reportes de administración deberán incluir dichos elementos.

- **Control presupuestario:** El **LICITANTE** adjudicado con base en las solicitudes de servicio que se presenten durante la vigencia del contrato respectivo y la atención brindada a las mismas, incluyendo las cancelaciones correspondidas, realizará un informe analítico del importe de los servicios devengados que incluya un desglose por cada tipo de servicios en relación con los montos y máximos establecidos en dicho instrumento jurídico; lo anterior, a efecto de facilitar las actividades de verificación de los consumos presentados y tener un control presupuestario de los mismos. En este componente se incluirán también aquellos documentos impresos o electrónicos que incidan en este rubro tales como: tendencias en el consumo financiero, ejercicio presupuestal por dirección normativa, por aplicativo y por tipo de tecnología, esto es detallado por centro de costos, servicios devengados, control de saldos presupuestales (pasivos) y proyecciones presupuestales, entre otros.

- **Aspectos técnicos y metodológicos de los entregables:** El **LICITANTE** adjudicado identificará y relacionará los elementos especificados en el contrato y sus anexos conforme a los cuales deberán presentarse los servicios considerando los entregables pactados, desde una perspectiva técnica y metodológica. Conforme a lo anterior, se incluirá en los reportes un informe que contenga los elementos exigidos en el contrato y sus anexos, con los cuales deberá acreditarse la entrega o prestación de los servicios. Identificando, entre otros elementos: (i) forma; (ii) plazos, (iii) servidores públicos responsables de la recepción, sus cargos y ubicaciones; (iv) lugares de entrega o prestación de servicios; (v) procedimiento para la suscripción de las actas; (vi) documentación de soporte solicitada que acredite fehacientemente la entrega de los servicios devengados de conformidad con la funcionalidad solicitada así como los niveles de servicio establecidos, y en su caso la propuesta de la posible aplicación de penas convencionales y deductivas, entre otros elementos

ANEXOS
DIVISIÓN DE CONTRATOS

- **Esquema de integración de pagos:** El **LICITANTE adjudicado** incluirá en los reportes la identificación de los elementos justificativos y comprobatorios que soporten la prestación de servicios durante el periodo que se reporte, conforme a las disposiciones normativas vigentes. Con esta información, el **LICITANTE** integrará la carpeta que soporte la solicitud de pago ante el **IMSS** por la entrega o prestación de los servicios devengados en el periodo mensual correspondiente, para su trámite y gestión por parte del Administrador del contrato, en términos de las facultades con que cuenta para la aceptación de los servicios.

- **Proyección del consumo de los servicios**: Con base en las facturas identificadas para pago, el **LICITANTE adjudicado** elaborará un modelo gráfico y analítico que registre el consumo mensual real de cada uno de los servicios facturados y que permita un análisis comparativo respecto al consumo programado, a efecto de brindar al administrador del contrato información para la toma de decisiones.

Los reportes de administración para la gestión del conocimiento administrativo de los servicios deberán formar parte invariablemente de los documentos justificativos que soportan cualquier pago que se realice durante la vigencia del contrato correspondiente.

8. Administradores del contrato

El Instituto designará a los Administradores del Contrato, mismos que conforme a sus atribuciones serán los encargados de verificar que los servicios que administran se entreguen en los tiempos y las formas establecidos en el Anexo Técnico.

9. Derechos de Autor

El **LICITANTE adjudicado** deberá presentar escrito, a más tardar a los 05 (cinco) días naturales del acto de fallo, en el que se obliga a liberar al Instituto de toda responsabilidad de carácter civil, mercantil, penal o administrativa que, en su caso, se ocasione con motivo de la infracción de derechos de autor, patentes, marcas u otros derechos de propiedad industrial o intelectual a nivel nacional o internacional, además de no encontrarse en ninguno de los supuestos de infracción a la Ley Federal de Derechos de Autor, ni a la Ley de la Propiedad Industrial.

En el entendido de que en caso de que sobreviniera alguna reclamación en contra del Instituto, por cualquiera de las causas antes mencionada, el prestador del servicio se compromete a llevar a cabo las acciones necesarias para garantizar la liberación del Instituto de cualquier controversia o responsabilidad de carácter civil, mercantil, penal o administrativa, que en su caso, se ocasione.

10.Confidencialidad

Las partes convienen en considerar como confidencial todos los datos contenidos en:,cintas magnéticas, programas de cómputo, disquetes o cualquier otro material que contenga información jurídica, operativa, técnica, financiera o de análisis, registros, documentos, especificaciones, productos, informes, dictámenes y desarrollos a que tenga acceso o que le sean proporcionados por Instituto.

De igual forma, será considerada como confidencial aquella información proporcionada por el Instituto para la ejecución del servicio que preste el **LICITANTE** adjudicado y sea propiedad exclusiva del Instituto.

Por lo anterior, el **LICITANTE** adjudicado reconoce que queda prohibida su difusión total o parcial en su favor o de terceros ajenos a la relación contractual, por cualquier medio, entre otros de

manera enunciativa más no limitativa: vía oral, impresa, electrónica, magnética, y en general por ningún medio, conforme el plazo señalado en el artículo 15 de Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

En este sentido, acepta que la prohibición señalada en el párrafo anterior, comprende inclusive, en forma enunciativa, que no se podrá llevar a cabo la difusión de la información del Instituto con fines de lucro, comerciales, académicos, educativos o para cualquier otro ajeno al objeto de la presente contratación, por lo que se responsabiliza del uso y cuidado de la información.

Por lo expuesto, el **LICITANTE** adjudicado se obliga a lo siguiente:

1) Mantener absoluta confidencialidad de la información a la cual tenga acceso, siendo responsable de que cada uno de los integrantes del personal asignado para el desarrollo y operación del proyecto, respetará el manejo correcto de la información.
2) Toda la información a que tenga acceso el personal que el **LICITANTE** adjudicado designe para la prestación de los servicios materia del presente proceso de contratación , es considerada de carácter confidencial, por lo que el **LICITANTE** adjudicado deberá garantizar que por ningún motivo se viole ninguno de los siguientes acuerdos:

    a. La información del IMSS y a la cual tenga acceso el personal del **LICITANTE** adjudicado, no deberá ser copiada o respaldada en ninguno de los equipos del personal del **LICITANTE** adjudicado sin autorización previa del Administrador del Contrato dentro del ámbito de su competencia.
    b. El acceso a la información del IMSS sólo podrá ser por personal del **LICITANTE** adjudicado, sólo podrá ser por parte del personal autorizado por el Administrador del Contrato dentro del ámbito de su competencia.
    c. De no cumplir con alguna de estas premisas, se considerará como una falta al acuerdo de confidencialidad que aceptó el **LICITANTE** adjudicado.

Cualquier persona que tuviera acceso a dicha información deberá ser advertida de lo convenido en este contrato, comprometiéndose a observar y cumplir lo acordado.

Ambas partes convendrán en que no será considerada como sujeta a las obligaciones de confidencialidad la siguiente documentación o información:

a) Aquella que sea conocida públicamente.
b) La que haya sido puesta a disposición de las partes por un tercero, antes de la fecha de celebración del presente contrato en forma confidencial.
c) La que haya sido desarrollada independientemente o adquirida por cualquiera de las partes, sin violar las estipulaciones del presente contrato o la que genere o desarrolle el posible proveedor en sus centros de desarrollo.
d) Aquella cuya revelación haya sido aprobada previamente por escrito.
e) La que de acuerdo a la Ley u orden judicial o administrativa, deba ser suministrada a terceras personas.

El uso de la información confidencial no otorgará a ninguna de las partes la titularidad o derechos de autor de la otra.

ANEXOS
DIVISIÓN DE CONTRATOS

11.Conformación de la Propuesta

Los participantes en el presente contratación, deberán entregar, de manera obligatoria, la Propuesta Técnica para realizar la respectiva evaluación de cada posible proveedor.

La Propuesta Técnica se presentará, tanto en formato impreso como en formato electrónico. En caso de que el Instituto detecte alguna diferencia entre la copia física y la electrónica, se considerará como elemento genuino el contenido del documento físico, siempre y cuando cumpla con los requisitos mencionados más adelante.

A continuación se puntualizan para su mejor atención los elementos, formatos y contenidos prioritarios para que la Propuesta Técnica pueda ser evaluada:

Presentación Física de la Propuesta Técnica

Los **LICITANTES** integrarán en su propuesta técnica algunos elementos, indispensables y con carácter de obligatorio, los cuales serán considerados por el Equipo Técnico designado por el Instituto durante la evaluación de las mismas. Las Propuestas Técnicas deben estar debidamente organizadas en carpetas, foliadas e incluirse un índice que indique clara y exactamente en dónde inicia y en dónde termina cada uno de los apartados y entregables correspondientes, para que el Equipo Técnico designado las revise ordenadamente. La propuesta técnica no es limitativa en alcance y extensión a los elementos aquí solicitados, sin embargo éstos son obligatorios de acuerdo a lo explicado en este documento.

Los participantes presentarán la propuesta técnica (en el caso de la impresa), debidamente organizada en las carpetas duras, separando las hojas en las carpetas por temas y/o capítulos, y también foliando las hojas de manera obligatoria desde la primera hasta la última en cada carpeta, para un mejor control del proceso de revisión técnica de las mismas. Cada carpeta debe contener tanto en su portada exterior, como en el lomo, un indicador que permita conocer el nombre del posible proveedor, el número de la carpeta, el identificador del proceso de contratación, y cualquier dato adicional que considere conveniente colocar y que apoye en la identificación del orden en que se integran. En la primera carpeta, además, el posible proveedor entregará un índice general de la información que entrega en cada carpeta, independientemente de los índices específicos de cada una de las carpetas.

Para el caso de la Propuesta Técnica electrónica, se solicita que dicha entrega se realice a través de medios ópticos (CD o DVD), o mediante dispositivos de almacenamiento tales como memorias tipo USB, todos estos deben estar debidamente protegidos mediante cajas de plástico o equivalentes, etiquetados e identificados con el nombre del **LICITANTE**, el número del medio óptico (en caso de ser más de uno), el identificador del procedimiento de contratación, y cualquier dato adicional que considere conveniente asentar de manera visible. El **LICITANTE** debe asegurarse de que el medio óptico pueda ser leído en lectores de disco convencional y que ha sido correctamente grabado. Puede incluir como respaldo, si así lo desea, módulos de memoria extraíbles o similares además del medio óptico.

El formato de archivos a almacenar de forma electrónica para la Propuesta Técnica, puede ser cualquiera de los siguientes:

- Microsoft Office Word
- Microsoft Office Excel
- Microsoft Office Poder Point
- PDF Postscript (Que permita la búsqueda de textos)
- Microsoft Office Visio

- Microsoft Office Project
- Formatos de imagen convencional (JPG, BMP, GIF, TIFF) para imágenes que no tengan una parte significativa de texto

Lenguaje

El **LICITANTE** será responsable de entregar su propuesta técnica preferentemente en lenguaje español. Sin embargo, dada la naturaleza del proyecto y de los servicios que se administrarán, se permitirá el uso de anglicismos generalmente aceptados en la industria, en aquellos términos que sean de origen extranjero, o que representen nombres de tecnologías particulares, sin embargo, incluirá el glosario de términos para su mejor comprensión.

En los casos donde así se indique, o que el **LICITANTE** juzgue necesario, será responsable de entregar documentación completa y detallada de los puntos en cuestión.

En los casos en los que esta documentación, sólo esté disponible en idioma inglés, se permitirá que el **LICITANTE** traduzca sólo el párrafo(s) que es de interés para el punto que se está documentando o citando, siempre y cuando el **LICITANTE** haga entrega del resto de la documentación en su formato e idioma original. Esta excepción sólo se hará para aquellos casos en donde la documentación requerida esté originalmente redactada en idioma inglés, y no se aceptarán propuestas que incluyan secciones de la documentación en ningún otro idioma que no sea inglés o español.

Diagramas

Todos los diagramas que formen parte de la propuesta técnica deben estar diseñados en Microsoft Visio o herramienta similar, y cada página estará debidamente rotulada, incluyendo el nombre del proyecto, el título del gráfico y el número de diagrama o figura.

Estos diagramas, junto con el resto de la presentación se entregarán en formato electrónico además del original en papel.

Información que debe contener la Propuesta Técnica

Los **LICITANTES** integrarán dentro de su propuesta técnica todos los entregables que a continuación se describen. Estos requisitos serán indispensables para verificar su capacidad operativa, tecnológica y técnica, para llevar a cabo satisfactoriamente la administración, operación, soporte e implementación de los servicios descritos en el Anexo Técnico correspondiente.

Los siguientes elementos son prioritarios e indispensables, por lo que se solicita a los participantes que en su propuesta incluya en carpetas, todos y cada uno de los entregables listados en la tabla siguiente, indicando correctamente la ubicación de cada uno de los siguientes rubros, para su fácil identificación y revisión, indicando el número identificador (ID) que aparece en la siguiente tabla:

No	Entregable
01	Aceptación de la totalidad de los capítulos y secciones contenidos en el Anexo Técnico correspondiente y Términos y Condiciones, para lo cual los participantes debe emplear el mismo orden y secuencia de temas que comprenden dichos documento, para manifestar su aceptación y compromiso explícito en todas y cada una de las solicitudes efectuadas como parte de los servicios, incorporando la glosa original del Anexo Técnico correspondiente para evitar ambigüedades en la suscripción.

ANEXOS

No	Entregable
02	Descripción a alto nivel de la arquitectura global que el **LICITANTE** utilizará para prestar los servicios objeto del Anexo Técnico correspondiente, apegándose a requerimientos del mismo. Este documento debe describir de forma general, las características de los componentes necesarios para entregar cada uno de los servicios, así como la estrategia que empleará para ajustarse al Plan General de Trabajo, pudiendo apoyarse para consolidar un documento concreto y conciso, en esquemas, diagramas, tablas, listados o cualquier elemento didáctico que el **LICITANTE** considere que aporta valor, para que el equipo técnico que el IMSS designe para la revisión de las propuestas, entienda los componentes, los servicios asociados, los procesos de servicio y sus características.
03	Manifestación escrita, firmada por el Representante Legal de la empresa participante, en la que establezca que cuenta con el soporte de los fabricantes de los Componentes Habilitadores de hardware y software ofertados, así como de los diferentes elementos de infraestructura auxiliar que incluya y que formen parte de la solución y; que cuenta con personal calificado para la prestación de los servicios ofertados.
04	Manifestación escrita, firmada por el Representante Legal de la empresa participante, en la que establezca que cuenta con el personal calificado y certificado de acuerdo a lo especificado en el Anexo Técnico correspondiente, de la solución tecnológica propuesta sobre los diferentes componentes que formen parte de su solución para la prestación de los servicios objeto del presente procedimiento de contratación.
05	Manifestación por escrito, firmada por el representante legal de la empresa participante, en la que expresa que los servicios ofertados cumplen con normas de calidad para la prestación de los servicios (Normas Oficiales Mexicanas, Normas Mexicanas, Normas Internacionales o las Normas de Referencia Aplicables; o las normas propias de calidad de la empresa) debiendo enunciarlas, de acuerdo a los artículos 20 Fracción VII, 53, 55 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público , 31 de su Reglamento, y 67 de la Ley Federal sobre Metrología y Normalización.
06	Manifestación por escrito, firmada por el representante legal de la empresa participante, en la que expresa que el personal encargado de la administración del proyecto acredita la certificación en PMI (cuando menos, certificado Profesional en Dirección de Proyectos [PMP] emitido por el Project Management Institute), incluyendo copia de la acreditación correspondiente.
07	Manifestación por escrito, firmada por el representante legal de la empresa participante, en la que expresa que cuenta en su plantilla de personal, con trabajadores con estudios a nivel licenciatura (título y cédula profesional), en carreras afines o relacionadas con la operación y administración de tecnologías de la información y comunicaciones. En caso de ser emitidos por una institución fuera de territorio nacional, se deberá presentar el apostille correspondiente.
08	Manifestación escrita, firmada por el Representante Legal de la empresa participante, cuenta con las certificaciones mencionadas en su propuesta.

12.Garantías

Garantía de cumplimiento de contrato

El LICITANTE adjudicado para garantizar el cumplimiento de todas y cada una de las obligaciones estipuladas en el contrato adjudicado, deberá presentar en la División de Contratos dependiente de la Coordinación Técnica de Contratos e Investigación de Mercados, de la Coordinación de Adquisición de Bienes y Contratación de Servicios de la entidad contratante, póliza de fianza en la misma moneda en que se cotizó el servicio, expedida por afianzadora debidamente constituida en términos de la Ley Federal de Instituciones de Fianzas, dentro de los 10 (diez) días naturales siguientes a la firma del contrato respectivo, para garantizar el cumplimiento de todas y cada una de las obligaciones a su cargo derivadas del contrato, a favor del IMSS, por un monto equivalente al 20% (veinte por ciento) sobre el importe total adjudicado, sin incluir el I.V.A. y/o IEPS, según sea el caso, en moneda nacional, de conformidad con lo establecido en el artículo 48 y 49 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como del 103 de su Reglamento y numeral 5.5.5.1 de las Políticas Bases Lineamientos en Materia de Adquisiciones, Arrendamientos y Prestación de Servicios del Instituto Mexicano del Seguro Social y demás disposiciones legales y normatividad aplicable en la materia, la cual será divisible en caso de presentarse algún incumplimiento.

La garantía de cumplimiento a las obligaciones del contrato, únicamente podrá ser liberada mediante autorización que sea emitida por escrito, por parte del Instituto en forma inmediata, siempre y cuando el LICITANTE adjudicado haya cumplido a satisfacción del Instituto con todas las obligaciones contractuales, para lo cual deberá presentar mediante escrito la solicitud de liberación de la fianza en la División de Contratos.

Ejecución de la garantía

Se hará efectiva la garantía relativa al cumplimiento del contrato:

- Cuando el **LICITANTE** adjudicado incumpla con cualquiera de las obligaciones establecidas en el contrato que se celebre.
- Cuando se rescinda administrativamente el contrato.

La ejecución de las garantías será con independencia de la aplicación de las penas convencionales y deducciones que procedan y de la rescisión administrativa del contrato.

Además de las sanciones anteriormente mencionadas, serán aplicables las que estipulen las disposiciones legales vigentes en la materia.

La ejecución de la garantía de cumplimiento del contrato, será proporcional al monto de las obligaciones incumplidas.

Garantía de Servicios.

Respecto de Garantías de Servicio, los posibles proveedores deberán presentar en su Propuesta Técnica, la documentación necesaria para garantizar el soporte de los fabricantes involucrados en la provisión de sus servicios; a fin de lograr los Niveles de Servicio requeridos en el Anexo Técnico correspondiente.

ANEXOS
DIVISIÓN DE CONTRATOS

13. Niveles de Servicio

El Servicio de Continuidad de la Nube IMSS 2020 se sujetará a los niveles de servicio establecidos en el apéndice respectivo del Anexo Técnico correspondiente.

14. Penas convencionales y Deductivas

- Los Administradores del Contrato serán los responsables de calcular y aplicar las penas convencionales y deductivas, previstas en el contrato o en el Anexo Técnico correspondiente, así como de notificarlas al prestador del servicio para que éste realice el pago correspondiente.

- En cualquier caso, las penas y deductivas no podrán exceder del monto de la garantía de cumplimiento del contrato.

- Las penas convencionales deben aplicarse bajo el principio de proporcionalidad, toda vez que si una parte de la obligación fue cumplida, la pena no puede ser aplicada a la totalidad del monto contratado.

15. Acuerdos de Niveles Operacionales

Con el objeto de garantizar la operación de los servicios, y de acuerdo con la metodología de administración de Niveles de Servicio ofertada, el **LICITANTE** adjudicado formalizará los Acuerdos de Nivel de Operación (OLA's) necesarios con el Instituto y con las entidades (terceros) involucradas en la provisión y uso de los servicios que demanda el presente proyecto, en coordinación con el Administrador del Contrato respectivo. Dichas entidades de terceros pueden entenderse también como otros proyectos o proveedores que fungen como componentes de la infraestructura habilitadora de los servicios objeto de este documento. Los OLAs se firmarán entre el Administrador del Contrato, en conjunto con el **LICITANTE** adjudicado y los demás administradores de contratos y/o servicios del Instituto con sus respectivos prestadores de servicios.

Los objetivos de los Acuerdos de Nivel de Operación son, de manera enunciativa más no limitativa, los siguientes:

- Definir y presentar los catálogos de servicio de distintos servicios, para identificar la participación de las diferentes áreas y prestadores de servicios de la organización para la entrega de los mismos.
- Delimitar las funciones del **LICITANTE** adjudicado y del personal que ejecuta los procesos de Negocio por parte del Instituto.
- Delimitar las funciones entre el **LICITANTE** adjudicado y otros prestadores de servicio que prestan servicios al Instituto, acordando un punto de demarcación definido por el alcance de los servicios señalados en el Anexo Técnico correspondiente; protegiendo ante cualquier circunstancia la continuidad de la operación del Instituto.
- Delimitar las funciones entre los prestadores de servicios actuales del Instituto que aún mantienen garantías vigentes de cualquier tipo de activo tecnológico en el alcance de este proyecto.

El **LICITANTE** adjudicado, entendido por el Instituto como un socio estratégico de su operación de TI y de los procesos de Negocio que son sustentados, así como los otros prestadores de servicios del Instituto, involucrados en dichos procesos de operación, trabajarán en conjunto para determinar los requerimientos y cumplir los compromisos que entre ellos se deriven a partir de los Acuerdos de Nivel de Operación.

0171

16.Ubicaciones para la prestación del servicio

El **LICITANTE** adjudicado tiene la obligación de prestar sus servicios en la ubicaciones declararas en el anexo técnico, apéndices y el presente documento o en las nuevas ubicaciones que el Instituto defina durante la vida del contrato resultante de este proceso, ya sea incrementando o sustituyendo alguna de las ubicaciones existentes, con objeto de acondicionar los servicios necesarios para su adecuado funcionamiento.

17.Consideraciones para la finalización del contrato

El **LICITANTE** adjudicado deberá tomar en cuenta, desde el arranque de la prestación de servicios, las medidas de previsión necesarias para cumplir con los requisitos señalados de manera referencial en éste apartado, verificados en la etapa final del servicio.

Tres (3) meses antes de la fecha de finalización del contrato y con el objeto de preparar el escenario para la continuidad operativa de los servicios objeto del Anexo Técnico correspondiente, el **LICITANTE** adjudicado comenzará a conformar y actualizar la documentación necesaria del proyecto, para que el Instituto pueda planear la Continuidad Operativa del servicio.

La documentación deberá incluir la información que se generó durante la vigencia del contrato, debidamente actualizada, tomando en consideración los eventos de administración de cambios y configuración, incidentes y problemas.

El **LICITANTE** entregará toda la información obligatoria así como los productos de trabajo referente al contrato, que el instituto requiera como parte del proceso de cierre. La información al cierre del contrato puede ser, de manera enunciativa más no limitativa la siguiente: memorias técnicas, arquitectura de los servicios, inventarios de software, infraestructura, CMDB, información de la Mesa de Ayuda, entre otros.

18.Pago de los Servicios

El pago de los Servicios descritos en el Anexo Técnico correspondiente, serán de manera "Mensual" para los servicios recurrentes, por "Evento" para los que sean solicitados a discreción del Instituto y por "Única Ocasión", para los servicios que están planificados como única vez en la vida del contrato.

El **LICITANTE** adjudicado reportará y solicitará al Instituto el pago asociado a los servicios que haya entregado o que hayan sido consumidos, conforme a las especificaciones descritas en el Anexo Técnico correspondientes, con estricto apego a las características y niveles de servicio que se requieren para cada rubro definido en el catálogo de servicios, y que cumplan con los aspectos generales de su operación; sujeto a posibles deducciones por incumplimiento de los mismos, por lo que el Instituto; a través del Administrador del Contrato, evaluará y dictaminará las condiciones de funcionalidad, operatividad y consumo de los servicios que sean entregados por el LICITANTE adjudicado para que proceda el pago mensual que debe efectuarse por los mismos.

El **LICITANTE** adjudicado deberá presentar ante el respectivo Administrador del Contrato, la documentación comprobatoria (entregables) y Acta de Aceptación del Servicio, con la que acreditará fehacientemente que se ha proporcionado el servicio a entera satisfacción del Instituto, y en estricto apego al procedimiento administrativo vigente en el Instituto. Dichos servicios deberán sustentarse mediante la entrega documental al Instituto.

ANEXOS

DIRECCIÓN DE CONTRATOS

El **LICITANTE** adjudicado entregará oportunamente la factura por los servicios del mes, en la Coordinación de Servicios Administrativos de la Dirección de Innovación y Desarrollo Tecnológico, así como la nota de crédito respectiva, en caso de que aplique, para que sean debidamente sancionadas, de acuerdo con los requisitos fiscales que establece el artículo 29-A del Código Fiscal de la Federación.

El **LICITANTE** adjudicado expedirá sus facturas en el esquema de facturación electrónica CFDI (Comprobantes Fiscales Digitales por Internet). La recepción de las mismas será a través del Portal de Servicios a Proveedores, y deberán ser proporcionadas en su formato XML. La validez de las mismas será determinada durante la carga y únicamente las facturas físicamente válidas serán procedentes para pago. El **LICITANTE** adjudicado deberá proporcionar a los Administradores del Contrato una representación impresa de la misma que cumpla con las especificaciones normadas por el Servicio de Administración Tributaria (SAT). La representación impresa por sí misma no será sustento para pago si no se hace la carga del XML del cual se originó, o si la misma no es una representación fiel del XML origen.

Las facturas deberán reunir los requisitos fiscales establecidos en la Ley de la materia, indicando los servicios prestados, así como el número de contrato. Una vez validada la documentación anterior y previo cotejo con la coordinación responsable, se procederá a la liberación de la factura y documentación soporte del LICITANTE adjudicado, para que éste la entregue ante la División de Trámite de Erogaciones, en las oficinas que determine para tal efecto el Instituto.

En caso de que el **LICITANTE** adjudicado presente su factura con errores o deficiencias, conforme a lo previsto en el artículo 90 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el Instituto, dentro de los 3 (tres) días hábiles siguientes a la recepción, indicará por escrito al participante ganador las deficiencias que se deberán corregir.

El pago se realizará mediante transferencia electrónica de fondos, a través del esquema electrónico interbancario que el IMSS tiene en operación, a menos que el **LICITANTE** adjudicado en forma fehaciente la imposibilidad para ello.

El pago se depositará en la fecha programada de pago, si la cuenta bancaria del **LICITANTE** adjudicado está contratada con BANAMEX, HSBC, BANORTE, SANTANDER o SCOTIABANK, si la cuenta pertenece a un banco distinto a los mencionados, el IMSS realizará la instrucción de pago en la fecha programada, y su aplicación se llevará a cabo el día hábil siguiente, de acuerdo con lo establecido por el CECOBAN.

El pago se realizará en los plazos normados por la Dirección de Finanzas, en el "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago", sin que éstos rebasen los 20 (veinte) días naturales posteriores a aquel en que el prestador del servicio presente en la División de Trámite de Erogaciones del Instituto, ubicada en Gobernador Tiburcio Montiel Número 15, Colonia San Miguel Chapultepec, Código Postal 11850, Delegación Miguel Hidalgo, México Distrito Federal, en días y horas hábiles.

Las facturas que amparen los servicios cuya recepción no genere alta a través del SAI ni realice enlace al PREI de manera electrónica, deberán contener la firma de recepción y de autorización para el trámite de pago, de acuerdo a lo establecido en el Procedimiento para la recepción, glosa y aprobación de documentos para trámite de pago vigente.

En caso de que el **LICITANTE** adjudicado celebre contrato de cesión de derechos de cobro, deberá notificarlo por escrito al Instituto, con un mínimo de 05 (cinco) días naturales anteriores a la fecha de pago programado, entregando invariablemente una copia de los contra-recibos cuyo importe se cede. Además de los documentos sustantivos de dicha cesión, el mismo procedimiento aplicará en el caso de que el **LICITANTE** adjudicado celebre contrato de cesión de derechos de

0172

cobro a través de factoraje financiero conforme al Programa de Cadenas Productivas de Nacional Financiera, S.N.C., Institución de Banca de Desarrollo.

El pago de los servicios quedará condicionado proporcionalmente al pago que el **LICITANTE** adjudicado deba efectuar por concepto de deducciones y penas convencionales por atraso.

Los impuestos y derechos que procedan con motivo de los servicios objeto de la presente adjudicación, serán pagados por el **LICITANTE** adjudicado, de conformidad a la legislación aplicable en la materia. El Instituto sólo cubrirá el impuesto al valor agregado (IVA) de acuerdo a lo establecido en las disposiciones legales vigentes en la materia.

El **LICITANTE** adjudicado deberá generar dichas facturas por periodos mensuales vencidos de servicio, y las entregará al Instituto en los primeros diez días naturales del mes siguiente al que se factura, de acuerdo con lo siguiente:

a) El **LICITANTE** adjudicado entregará la factura a la Coordinación de Servicios Administrativos de la DIDT.
b) La Coordinación de Servicios Administrativos enviará la factura a la Coordinación de Sistemas de Infraestructura Tecnológica Institucional para su trámite en términos del contrato.
c) La Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI) enviará al respectivo Administrador del contrato, la citada factura con la petición de que proceda a la validación de los servicios comprendidos en la misma, en su caso, emita la aceptación a entera satisfacción de los servicios.
d) Los Administradores del Contrato integrarán los respectivos sustentos documentales incluyendo los resultados del cálculo de las métricas de los niveles de servicio establecidos en el Anexo Técnico para la aplicación de deducciones y penas convencionales conducentes enviándola a la Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI).
e) La Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI) valida y enviará la documentación completa a la Coordinación de Servicios Administrativos para la gestión de pago.
f) La Coordinación de Servicios Administrativos entregará la factura al LICITANTE adjudicado.
g) El **LICITANTE** adjudicado deberá ingresar su factura y documentación al área de Trámite de Erogaciones para los trámites correspondientes.

19.Mecanismos de control para la administración del contrato

Rescisión administrativa del contrato.

En términos de lo dispuesto en el artículo 54, de la LAASSP, el Instituto podrá rescindir administrativamente el contrato en cualquier momento, cuando el **LICITANTE** adjudicado, incurra en incumplimiento de cualquiera de las obligaciones a su cargo, de conformidad con el procedimiento siguiente.

Si el Instituto considera que el **LICITANTE** adjudicado ha incurrido en alguna de las causales de rescisión que se consignan más adelante, lo hará saber al **LICITANTE** adjudicado, de forma indubitable por escrito, a efecto de que éste exponga lo que a su derecho convenga y aporte, en su caso, las pruebas que estime pertinentes, en un término de 5 (cinco) días hábiles, a partir de la notificación de la comunicación de referencia.

Transcurrido el término a que se refiere el párrafo anterior, el Instituto contará con un plazo de quince días para resolver, considerando los argumentos y pruebas que hubiere hecho valer el **LICITANTE** adjudicado. La determinación de dar o no por rescindido el contrato deberá ser debidamente fundada, motivada y comunicada al **LICITANTE** adjudicado dentro dicho plazo.

ANEXOS
DIRECCIÓN DE CONTRATOS

En caso de que el Instituto, determine dar por rescindido el contrato, se deberá formular y notificar un finiquito dentro de los 20 (veinte) días naturales siguientes a la fecha en que se notifique la rescisión, de conformidad con el artículo 99, del Reglamento de la LAASSP, en el que se hagan constar los pagos que, en su caso, deba efectuar el Instituto, por concepto del servicio, proporcionado por el **LICITANTE** adjudicado, hasta el momento en que se determine la rescisión administrativa.

En el supuesto de que se rescinda el contrato, el Instituto, no aplicará las penas convencionales, ni su contabilización, para hacer efectiva la garantía de cumplimiento de este instrumento jurídico. Iniciado un procedimiento de conciliación el Instituto, bajo su responsabilidad podrá suspender el trámite del procedimiento de rescisión.

Si previamente a la determinación de dar por rescindido el contrato, **LICITANTE** adjudicado, está en condiciones óptimas para continuar proporcionando el servicio, el procedimiento iniciado quedará sin efectos, previa aceptación y verificación del Instituto, por escrito, de que continúa vigente la necesidad de contar con los servicios, en su caso, las penas convencionales correspondientes.

El Instituto, podrá determinar no dar por rescindido el contrato, cuando durante el procedimiento advierta que dicha rescisión pudiera ocasionar algún daño o afectación a las funciones que tiene encomendadas. En este supuesto, el Instituto, elaborará un dictamen en el cual justifique que los impactos económicos o de operación que se ocasionarían con la rescisión del contrato resultarían más inconvenientes.

De no darse por rescindido el contrato, el Instituto, establecerá de conformidad con el **LICITANTE** adjudicado, un nuevo plazo para el cumplimiento de aquellas obligaciones que se hubiesen dejado de cumplir, a efecto de que el **LICITANTE** adjudicado, subsane el incumplimiento que hubiere motivado el inicio del procedimiento de rescisión. Lo anterior, se llevará a cabo a través de un convenio modificatorio en el que se atenderá a las condiciones previstas en los dos últimos párrafos del artículo 52, de la LAASSP.

Cuando por motivo del atraso en la entrega de los bienes o la prestación de los servicios, o el procedimiento de rescisión se ubique en un ejercicio fiscal diferente a aquél en que hubiere sido adjudicado el contrato, la dependencia o entidad convocante podrá recibir los bienes o servicios, previa verificación de que continúa vigente la necesidad de los mismos y se cuenta con partida y disponibilidad presupuestaria del ejercicio fiscal vigente, debiendo modificarse la vigencia del contrato con los precios originalmente pactados. Cualquier pacto en contrario a lo dispuesto en este artículo se considerará nulo.

El Instituto podrá rescindir administrativamente el contrato sin más responsabilidad para el mismo y sin necesidad de resolución judicial, cuando el **LICITANTE** adjudicado incurra en cualquiera de las causales siguientes.

1. Cuando no entregue la garantía de cumplimiento del contrato, dentro del término de diez días naturales posteriores a la firma del mismo.
2. Cuando incurra en falta de veracidad total o parcial respecto a la información proporcionada para la adjudicación o formalización del contrato.
3. Sea declarado en concurso mercantil o cualquier situación análoga o equivalente que afecte el patrimonio del **LICITANTE** adjudicado.
4. Cuando de manera reiterativa y constante, **LICITANTE** adjudicado sea sancionado por parte del IMSS con penalizaciones sobre el mismo concepto de los servicios prestados y con ello se afecten los intereses del IMSS.
5. Si la Comisión Federal de Competencia, de acuerdo a sus facultades, notifica al Instituto la sanción impuesta al **LICITANTE** adjudicado, con motivo de la colusión de precios en que hubiese incurrido durante el procedimiento, en contravención a lo dispuesto en los artículos 9, de la Ley Federal de Competencia Económica y 34, de la LAASSP.

Terminación anticipada del contrato.

En términos de lo establecido en el artículo 54 Bis, de la LAASSP, el Instituto podrá dar por terminado anticipadamente el contrato sin responsabilidad para éste y sin necesidad de que medie resolución judicial alguna, cuando concurran razones de interés general o bien, cuando por causas justificadas se extinga la necesidad de requerir los bienes o servicios objeto del presente contrato, y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas se ocasionaría algún daño o perjuicio al Instituto, o se determine la nulidad de los actos que dieron origen al contrato, con motivo de la resolución de una inconformidad o intervención de oficio emitida por la Secretaría de la Función Pública (SFP). En estos casos el Instituto reembolsará al **LICITANTE** adjudicado, los gastos no recuperables en que haya incurrido, siempre que éstos sean razonables, estén debidamente comprobados y se relacionen directamente con la contratación del servicio motivo del presente procedimiento de contratación.

20.Responsabilidad

El **LICITANTE** adjudicado se obliga a responder por su cuenta y riesgo de los daños que sean determinados por la autoridad judicial competente que por inobservancia o negligencia de su parte, lleguen a causar al Instituto, con motivo de las obligaciones pactadas en este instrumento jurídico.

21.Responsabilidad Laboral

Queda expresamente estipulado que el personal para la prestación del servicio o que utilice el **LICITANTE** adjudicado para el cumplimiento de cualquiera de las obligaciones emanadas de este instrumento, estará bajo la responsabilidad única y directa de éste y por lo tanto, en ningún momento se considerará al Instituto como patrón sustituto o solidario, ni tampoco al **LICITANTE** adjudicado como intermediario, por lo que el Instituto no tendrá relación alguna de carácter laboral con dicho personal y consecuentemente queda liberado de cualquier responsabilidad laboral, fiscal, en materia de seguridad social, o de cualquier otra naturaleza jurídica, derivado de las disposiciones legales y demás ordenamientos en materia de trabajo y seguridad social, obligándose el **LICITANTE** adjudicado a responder de cualquier acción legal y/o reclamación que se pudiera presentar en contra del Instituto.

Independientemente de lo anterior, el **LICITANTE** adjudicado deberá de cumplir con las obligaciones en materia de seguridad social de sus trabajadores que van a prestar los servicios al Instituto, lo anterior en el marco de la Ley Federal del Trabajo vigente, en sus artículos 15-A, 15-B, 15-C y 15-D, por lo que "el Instituto" en cualquier momento podrá verificar su cumplimiento. Para lo cual el Instituto solicitará de manera mensual al proveedor el reporte mensual (Emisión IMSS).

ANEXOS

D. [illegible] N DE CONTRATOS

22.Firmas de elaboración, revisión y aprobación

Responsables de Elaboración

Héctor Martínez Valenzuela
Titular de la División de Telecomunicaciones
12/11/2019

Alejandro Paniagua Ramírez
Titular de la División de Administración de Riesgos Tecnológicos
12/11/2019

Carlos Francisco Ramírez del Rivero,
Titular de la División de Administración y Continuidad de la Operación
12/11/2019

Héctor Javier Reyes Oropeza
Titular de la División de Administración, Procesamiento y Almacenamiento
12/11/2019

Responsables de Revisión

Javier Cortés López
Titular de la Coordinación Técnica de Operación de Servicios Tecnológicos
12/11/2019

Carlos Calderón Zacarias
Titular de la Coordinación
Técnica de Redes y
Telecomunicaciones
12/11/2019

Responsables de Aprobación

Eduardo Oropeza Ortiz
Titular de la Coordinación de
Sistemas de Infraestructura
Tecnológica Institucional
12/11/2019

ANEXOS

DIVISIÓN DE CONTRATOS

SIN TEXTO

IMSS	**INSTITUTO MEXICANO DEL SEGURO SOCIAL** **DIRECCIÓN DE ADMINISTRACIÓN** **UNIDAD DE ADQUISICIONES E INFRAESTRUCTURA** **COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS** **COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS**	**Contrato Número** **P0M0026**

ANEXO 2

"PROPUESTA TÉCNICA, PROPUESTA ECONÓMICA Y ACTA DE ADJUDICACIÓN"

ANEXOS

DIVISÍON DE CONTRATOS

EL PRESENTE ANEXO CONSTA DE **43** HOJAS INCLUYENDO ESTA CARÁTULA

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

SIN TEXTO

ID	Nombre del Entregable	Descripción	Periodicidad	Compromiso de Entrega
1	Criterios de aceptación de los entregables asociados a la puesta en marcha y operación de los Servicios. Este entregable tendrá como alcance el formato estandarizado de todos los documentos que se entregan.	Documento que enumera los Criterios de Aceptación acordados durante el Arranque del Servicio, con los elementos propuestos por KIO NETWORKS para que el IMSS pueda avalar la entrega-recepción de los servicios prestados	Única Vez	15 días después del arranque del servicio
2	Plan de Mantenimientos Preventivos (Road Map) de las plataformas de cómputo y/o procesamiento.	Road Map anual de Mantenimientos Preventivos para garantizar la correcta operación de la infraestructura	Única Vez	30 días después del arranque del servicio
3	Categorizaciones para Mesa de Servicio de KIO NETWORKS	Documento con la categorización de solicitudes de cambios, incidentes y problemas durante la operación de los Servicios para garantizar la correcta implementación de su mesa de servicio.	Única Vez	30 días después del arranque del servicio
4	Proceso de Gestión de incidentes	Descripción del proceso que se llevará a cabo para la Gestión de Incidentes	Única Vez	30 días después del arranque del servicio
5	Proceso de Gestión de problemas	Descripción del proceso que se llevará a cabo para la Gestión de Problemas	Única Vez	30 días después del arranque del servicio
6	Proceso de Gestión de cambios	Descripción del proceso que se llevará a cabo para la Gestión de Cambios	Única Vez	30 días después del arranque del servicio
7	Inventario con el estado Actual de los Servicios	KIO NETWORKS identificará nuevamente y actualizar la matriz de Servicios Críticos.	Única Vez	Semestral

ID	Nombre del Entregable	Descripción	Periodicidad	Compromiso de Entrega
8	Monitoreo de Niveles del Servicio de Disponibilidad de la Infraestructura.	Herramienta que permita monitorear los niveles de servicio de la infraestructura crítica para la Operación de los Servicios del IMSS	En línea	60 días después del arranque del servicio
9	Reporte de Gestión de Requerimientos	Documento que contiene la volumetría mensual de las solicitudes (tickets) registrados en la herramienta de la mesa de servicio de KIO NETWORKS que se registran para la atención del instituto	Mensual	1 mes
10	Reporte de Gestión de Incidentes	Documento que contiene la volumetría de los incidentes presentados durante el mes	Mensual	1 mes
11	Documento con los casos de soporte solicitados hacia el fabricante del producto	Documento con el listado de casos reportados con los respectivos fabricantes de las soluciones tecnológicas, indicando el estado que guarda cada uno	Mensual	1 mes
12	Reporte Mensual de Activos para la Operación del Servicio	Reporte con el inventario de los activos que forman parte del ecosistema tecnológico utilizado para la entrega de los servicios	Mensual	1 mes
13	Reporte de Gestión de Eventos	Documento que contiene la volumetría de los eventos presentados durante el mes, agrupándolos los que tuvieron impacto.	Mensual	1 mes
14	Reporte de Gestión de Problemas	Documento que continúen la volumetría de los problemas registrados durante el mes.	Mensual	1 mes
15	Reporte de Gestión de Cambios.	Documento que continúen la volumetría de los cambios registrados durante el mes, así como su calendario y las afectaciones a los activos en la CMDB	Mensual	1 mes
16	Reporte de tickets generados	Documento que continúen la volumetría de los ticket's generados durante el mes	Mensual	1 mes

ANEXOS

DIVISÍON DE CONTRATOS

- Mes que se evalúa
- Cantidad total de acciones realizadas en el mes
- Cantidad total de acciones realizadas dentro de la ventana de tiempo establecida en el mes
- Anexo de relación de acciones realizadas, identificando su tipo, tiempo de inicio y finalización
- Valores esperados en el mes para cada Nivel de Servicio medido
- Valores obtenidos en el mes para cada Nivel de Servicio medido
- Diferencia entre el Valor esperado y el Valor obtenido
- Total del monto a penalizar en el mes.

10.4 Objetivos y Métricas específicas de Niveles de Servicio

KIO NETWORKS acepta lo descrito en el Apéndice denominado **"Objetivos y Métricas de Niveles de Servicio"** especifica con detalle las métricas, objetivos y los mecanismos y/o procedimientos de cálculo de los niveles de servicio para cada uno de los servicios descritos en la presente Propuesta Técnica.

11 DESCRIPCIÓN GENERAL DE ENTREGABLES

El Instituto requiere recibir distintos tipos de documentos o reportes, que favorezcan el desempeño y la continuidad del servicio, para que acrediten y de certidumbre a las actividades diarias que **KIO NETWORKS** efectuará bajo la supervisión del Instituto para tales efectos. Estos documentos no deben ser confundidos con aquellos que integran la Propuesta Técnica de **KIO NETWORKS** en el proceso de contratación, mismos que se describen con detalle en el apartado correspondiente de la convocatoria objeto de la presente Propuesta Técnica.

Para una mejor identificación, los entregables que **KIO NETWORKS** elaborará a lo largo de la vigencia del contrato, se dividen en aquellos que se efectúan "por única vez" y aquellos que se elaboran de manera periódica (mensual o bajo demanda).

Es importante destacar que la totalidad de los entregables que **KIO NETWORKS** efectúe, de acuerdo con las disposiciones descritas en el presente Anexo Técnico, estarán alineados a la normatividad vigente aplicable en el Instituto (MAAGTIC-SI). El Instituto podrá entregar a **KIO NETWORKS**, los formatos que a este respecto tenga en su poder para la elaboración de los documentos y reportes relacionados con los entregables, durante las Mesas de Trabajo de del Arranque del servicio.

KIO NETWORKS se compromete a entregar, de manera formal a lo largo de la vigencia del contrato, un conjunto de documentos relacionados a cada servicio requerido en el presente anexo técnico.

Cualquier entregable adicional a los listados a continuación y que no se encuentre en la descripción de los servicios de la presente Propuesta Técnica, y que **KIO NETWORKS** considere necesario para establecer para una relación más eficiente entre **KIO NETWORKS** y el Grupo de Gobierno de Contrato, será propuesto por **KIO NETWORKS**, revisado y en su aceptado por el GGC para optimizar el desempeño del servicio en su conjunto.

A continuación, se listan los entregables asociados a los servicios que requieren una especificación puntual, sin menos cabo de todos los entregables, productos de trabajo y cualquier obligación descrita en los servicios objeto de la presente Propuesta Técnica.

11.1 Entregables asociados a los Servicio de Continuidad de la Operación y Soporte

Núm.	Descripción	Periodicidad	Inicio de la entrega
	parcialmente detenida en un proceso de negocio).		
07	Reportes de Administración por Procesos: Administración de configuraciones. KIO NETWORKS debe entregar un reporte en donde se identifiquen las configuraciones y cambios que se hayan realizado a la infraestructura (actualización de la memoria técnica de los servicios).	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
08	Reportes de Administración por Procesos: Administración de Cambios KIO NETWORKS debe entregar un reporte en donde se identifiquen los cambios (RFCs) ejecutados. .	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
09	Reportes de Administración por Procesos: Administración de Problemas KIO NETWORKS debe entregar un reporte en donde se identifiquen los problemas identificados.	Se entregarán dentro de los primeros 10 días hábiles de cada mes devengado	Una vez iniciado el servicio
10	Reportes de utilización y desempeño. Deberá contener estadísticas principales de uso y desempeño, así como las tendencias de todos los componentes del servicio. Se acordará en la Planeación del Arranque el contenido de este tipo de reportes.	Se entregarán dentro de los primeros 10 días hábiles de cada mes vencido	Una vez iniciado el servicio
11	Reportes, informes o entregables descritos en las secciones de cada servicio	Se entregarán acorde a lo especificado en el apartado o en los tiempos definidos en las mesas de arranque.	Una vez iniciado el servicio

El detalle de los atributos, variables y formato de los reportes requeridos en este apartado y en general en los descritos en los apartados de la presente Propuesta Técnica, serán propuestos por **KIO NETWORKS** para la aprobación del Instituto durante las mesas de arranque. El Instituto podrá acordar con **KIO NETWORKS** modificaciones a los mismos.

Los reportes, entregables, productos de trabajo mencionados en este apartado y en general en los apartados descritos en los servicios de la presente Propuesta Técnica, serán atendidos por **KIO NETWORKS** bajo los siguientes lineamientos que se mencionan de manera enunciativa más no limitativa:

- Deberán entregarse con la periodicidad establecida en el presente anexo técnico, apéndices o en las mesas de trabajo.
- El Instituto podrá solicitar en cualquier momento, una copia en medio electrónico del contenido total o parcial de la información, misma que será entregada a más tardar 07 días hábiles después de su solicitud.

10.3.1 Consideraciones generales para los reportes de nivel de servicio

10.3.1.1 Disponibilidad

Reportes de cumplimiento de acuerdos de niveles de servicio establecidos para cada uno de los servicios de la presente Propuesta Técnica.

Reportes con diagramas, tablas e histogramas de distribución y sumarización del comportamiento global del servicio para los parámetros definidos en periodos de tiempo determinados por el Instituto.

Los reportes de niveles de servicio tendrán de manera enunciativa más no limitativa las siguientes características:

- Identificación del recurso
- Mes que se evalúa
- Valores esperados en el mes para cada Nivel de Servicio medido
- Valores obtenidos en el mes para cada Nivel de Servicio medido
- Diferencia entre el Valor esperado y el Valor obtenido
- Total del monto a penalizar en el mes

10.3.1.2 Entrega del servicio

Reportes de cumplimiento de acuerdos de niveles de servicio establecidos para cada una de las acciones concluidas en el mes bajo evaluación.

Reportes con diagramas, tablas e histogramas de distribución y sumarización del comportamiento global del servicio para los parámetros definidos anteriormente en periodos de tiempo determinados.

Los reportes de niveles de servicio tendrán las siguientes características mínimas:

ANEXOS

DIVISIÓN DE CONTRATOS

- Multiusuario
- Mantenimiento de respaldos
- Disponibilidad
- Repositorio de los reportes (digitalizados) a entregar durante el contrato

10.2 Definición General de Entrega

La entrega de los servicios administrados, como los descritos en el presente Anexo Técnico, se define como el evento de cumplimiento en la entrega del servicio ofrecido al Instituto por **KIO NETWORKS**.

Un evento será considerado como realizado satisfactoriamente cuando el Instituto, a través del personal y/o las áreas correspondientes, proporcionen retroalimentación o confirmación aprobatoria para su cierre. **KIO NETWORKS** y el Grupo de Gobierno del Contrato precisarán de manera formal en mesas de arranque, las políticas y evidencias de aceptación para cada tipo de entrega, los cuales podrán ser actualizados conforme a las necesidades del Instituto.

Se entiende por acción solicitada a cualquier evento, requerimiento, solicitud registrada y/o notificada de manera formal y oportuna por el Instituto hacia **KIO NETWORKS**, conforme al procedimiento y las herramientas establecidas para tal fin (Mesa de Servicio de **KIO NETWORKS** o Instituto, o cualquier otra definida en las mesas de arranque).

Dentro de la Entrega del Servicio, se incluye la atención de diferentes requerimientos, solicitudes, eventos, o situaciones que comprenderán varios tipos de esquemas de atención, a describirse dentro de cada sección especifica, dedicada a los diferentes servicios de la presente Propuesta Técnica.

10.3 Reportes del Servicio

Con el objeto de medir la entrega, disponibilidad y desempeño de los servicios proporcionados, **KIO NETWORKS** definirá y generará los reportes de niveles de servicio de los servicios solicitados, que serán parte de los entregables periódicos del servicio.

Los reportes serán generados con base en las herramientas habilitadas para tal efecto (en los casos que aplique) y ser entregados por **KIO NETWORKS** al Grupo de Gobierno del Contrato de la siguiente manera:

Tabla 3 Reportes de Niveles de Servicio

[illegible]	[illegible]	[illegible]	[illegible]
01	Reporte de nivel de servicio: Entrega del Servicio desglosado por tipo de servicio	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
02	Reporte de nivel de servicio: Disponibilidad desglosado por tipo de servicio	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
03	Reporte de nivel de servicio: Desempeño desglosado por tipo de servicio	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
04	Reporte de nivel de servicio: Impacto a la operación	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
05	Reporte de nivel de servicio: Atención de Solicitudes en la Operación del Servicio.	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
06	Reportes de Administración por Procesos: Incidentes y Problemas a) KIO NETWORKS debe entregar al Grupo de Gobierno del contrato reporte de análisis de cumplimiento de los tiempos de solución de incidentes. b) Para los incidentes de que dejen la operación detenida o parcialmente detenida, KIO NETWORKS entregará reporte técnico y ejecutivo. c) Por excepción el Instituto podrá solicitar los reportes anteriormente indicados para los incidentes de prioridad 3 (operación	a) Se entregarán dentro de los primeros 05 días hábiles de cada mes. b) Se entregarán 3 días hábiles después de haber concluido la atención del mismo. c) Se entregarán 5 hábiles después de haber concluido la atención del mismo.	Una vez iniciado el servicio

10 NIVELES DE SERVICIO

El proceso de Administración del Nivel del Servicio deberá involucrar tanto a **KIO NETWORKS** como al **IMSS** para mantener y monitorear el adecuado funcionamiento del servicio. **KIO NETWORKS** mantendrá una revisión continúa de los logros de servicio para garantizar que la calidad del servicio sea mantenida y mejorada permanentemente.

Nivel general de servicio

Los niveles de servicio establecidos que cumplirá **KIO NETWORKS** en la prestación de los servicios es el siguiente:

El nivel de servicio base para este contrato es de:

Nivel de Disponibilidad	Minutos indisponibles permitidos en el mes para los servicios del presente contrato
99.982% sobre la plataforma instalada (TIER III)	7.8 minutos

Esta disponibilidad establecida incluye el servicio de soporte técnico en caso de falla en un esquema de 7x24 en días y horarios hábiles con soporte presencial certificado, por lo que en su caso, será exigible la participación de especialistas únicamente en estos horarios, sin embargo, puede requerirse presencia en un esquema 7x24 del personal asociado al servicio, a petición del Instituto.

10.1 CATEGORÍAS DE NIVELES DE SERVICIO

Con el fin de lograr una administración más ágil se han clasificado los acuerdos de nivel de servicio en dos categorías:

La primera categoría hace referencia a los **niveles de servicio de gestión**, los cuales miden la calidad de la entrega y gestión de cada uno de los servicios del Anexo Técnico.

La segunda categoría está relacionada con los **niveles de servicio de infraestructura**, los cuales medirán la calidad de la disponibilidad y el desempeño de los componentes que integran los servicios del Anexo técnico.

El Instituto y **KIO NETWORKS** podrán generar métricas adicionales que, junto con las anteriores, las cuales servirán para medir el servicio proporcionado.

KIO NETWORKS incluirá en su propuesta técnica, la solución automatizada de medición de los diferentes niveles de servicio antes de su implementación, estableciendo claramente los elementos involucrados en el aprovisionamiento del servicio, las formas de medición, el método de tratamiento de la información generada para su consolidación, los reportes, estadísticas, documentación que será entregada, intervalos de medición y la forma como se harán disponibles los resultados al Grupo de Gobierno de Contrato para su dictamen consolidado.

KIO NETWORKS utilizará las herramientas habilitadas en el **Servicio de Continuidad Operativa y Soporte** como entrada de datos, así como herramientas utilizadas por el Instituto (BMC Remedy y/o cualquier otra que indique el Instituto) mismas que serán definidas en las mesas de arranque de contrato; así como proveer, instalar y habilitar la Infraestructura y el licenciamiento de su propia herramienta, incluyendo los elementos de hardware y software necesarios para el acopio, consolidación, explotación de información y generación de reportes e informes.

La herramienta de **KIO NETWORKS** estará accesible desde cualquier punto de la red del Instituto, con la finalidad de mostrar de forma clara y oportuna la información que soporta el nivel de servicio ofrecido, teniendo la posibilidad de contar con indicadores globales y consolidados dependiendo del tipo de métrica y también de observar el detalle que compone estos indicadores. Dicha infraestructura de hardware y software estará sujeta a los niveles de servicio descritos en el presente documento.

KIO NETWORKS proporcionará la transferencia de conocimiento y entrenamiento tecnológico necesario en el manejo y administración de las herramientas de niveles de servicio para al menos 20 personas, en las instalaciones que se acuerden con el Instituto. El calendario y fechas de la transferencia de conocimiento y entrenamiento tecnológico se impartirán durante las fechas acordadas en las mesas de arranque del servicio.

El software propuesto para niveles de servicio cumplirá al menos con los siguientes aspectos, mencionados de manera enunciativa más no limitativa:

- Acceso a las herramientas desde la red del Instituto e Internet
- Generación de reportes (Excel, RTF, PDF, etc.)
- Generación de Estadísticos (gráficas, dashboard)
- Medir los tiempos de atención
- Que se pueda importar y exportar información
- Consulta de información en tiempo real
- Contenga pistas de auditoría de cada evento
- Se pueda migrar de plataforma
- Contemple notificaciones electrónicas
- Ambiente gráfico

ANEXOS

DIVISIÓN DE CONTRATOS

actual y continuidad de la operación de servicios.		datos de **KIO NETWORKS** incluyendo servicios de punto neutro.	parte del IMSS, del Plan de Trabajo Detallado		
	7	Finalización de actividades de migración del centro de datos actual al centro de datos de **KIO NETWORKS** incluyendo punto neutro.	Plazo ofertado por **KIO NETWORKS**	Plazo ofertado por **KIO NETWORKS**	4
	8	Estabilización de los Niveles de Servicio a la finalización de la etapa de migración.	Plazo ofertado por **KIO NETWORKS**	Plazo ofertado por **KIO NETWORKS**	6 y 7
	9	Inicio de los Servicios asociados a la continuidad operativa de los servicios de la presente Propuesta Técnica.	Plazo ofertado por **KIO NETWORKS**	Plazo ofertado por **KIO NETWORKS**	N/A
	10	Actividades de Finalización del Contrato.	A más tardar 4 meses naturales antes del día de la Finalización del Contrato	31 de diciembre de 2020	N/A
CIERRE	12	Finalización del Contrato	-	31 de diciembre de 2020	N/A

KIO NETWORKS elaborará Programas de Trabajo Detallados que sean necesarios para la puesta a punto de cada uno de los servicios de:

- Servicio de Continuidad y Gestión de la Operación
- Servicio de Operación y Calidad de la Seguridad informática perimetral
- Servicio de Integralidad de ambientes distribuidos a nivel nacional y telecomunicaciones
- Servicio de Gestión de Medición del Desempeño de Aplicativos y Componentes Institucionales

9 CRONOGRAMA DE ACTIVIDADES

El Plan de Trabajo General especifica las fases más relevantes del contrato, KIO NETWORKS entregará el plan de trabajo y establecer los tiempos máximos que prevé emplear en cada una de ellas a fin de dar cumplimiento de las obligaciones relacionadas a los servicios de la presente Propuesta Técnica.

Ilustración 4 Marco de referencia del Plan de Trabajo General

KIO NETWORKS en su propuesta incluirá el Plan de Trabajo General, que deberá especificar hitos y fases para el cumplimiento de los servicios de la presente Propuesta Técnica, mismos que serán respetados en todo momento tanto en fechas y compromisos establecidos como en el alcance y funcionalidad ofertada. **KIO NETWORKS** integrará en su propuesta, las definiciones o peticiones de servicio que se establecen en esta Propuesta Técnica y que son vinculadas a una o más fases del Plan de Trabajo General.

A continuación, se especifica de manera enunciativa más no limitativa, una tabla-resumen de los hitos que se prevén en el Plan de Trabajo General para los servicios descritos en el presente anexo técnico, indicando Fase, Identificador del hito en cuestión (ID), el nombre o descripción del hito, las fechas relativas y absolutas de inicio y/o término, cantidad de días naturales máximos de duración por hito que **KIO NETWORKS** oferte.

Tabla 2 Hitos relevantes a considerar en el Plan de trabajo

Proceso de Migración de Centro de Datos actual al Servicio de Continuidad de Nube IMSS 2020.					
Planeación del Arranque	1	Kick-Off y presentación del equipo de trabajo de KIO NETWORKS.	A más tardar 10 días naturales posteriores al Fallo	Plazo ofertado por KIO NETWORKS	N/A
	2	Mesas (sesiones) de trabajo de Planeación del Arranque, entre KIO NETWORKS y el IMSS, convocadas por el Grupo Administrador del Contrato IMSS	Plazo ofertado por KIO NETWORKS	Plazo ofertado por KIO NETWORKS	1
	3	Presentación, por parte de KIO NETWORKS del Plan de Trabajo Detallado	A más tardar 5 días naturales posteriores a la finalización de las Mesas de Trabajo	Plazo ofertado por KIO NETWORKS	2
	4	Análisis y Revisión (en su caso aprobación) del Plan de Trabajo Detallado de parte del Grupo Administrador del Contrato del IMSS	A más tardar 15 días naturales posteriores a la entrega del Plan Detallado de parte de KIO NETWORKS	Plazo ofertado por KIO NETWORKS	8
	5	En caso de aplicar, incluir firma de Acuerdos de Nivel de Operación (OLAs) entre KIO NETWORKS y Terceros Involucrados en los servicios de la presente Propuesta Técnica.	A lo largo de los siguientes 25 días naturales a partir del Kick-Off del proyecto	Plazo ofertado por KIO NETWORKS	1
Actividades de migración de centro de datos	6	Inicio de actividades de migración del centro de datos actual al centro de	Al día natural siguiente a la aprobación, por	Plazo ofertado por KIO NETWORKS	4

ANEXOS

DIVISIÓN DE CONTRATOS

Asimismo, **KIO NETWORKS** proporcionará la representación gráfica y analítica de una línea de tiempo en el cual se detallen las fechas límite para el cumplimiento de obligaciones primarias y secundarias conforme a las órdenes de servicio y los plazos y procedimientos previstos en el contrato respectivo.

- **Análisis de consecuencias: KIO NETWORKS** realizará un análisis respecto de la aplicación del sistema de sanciones previsto en el contrato durante la vigencia del mismo, con base en las solicitudes u órdenes de servicio recibidas y la atención dada a las mimas. Con esta información el Administrador del Contrato efectuará las acciones de verificación que permitan la aplicación de las reglas de proporcionalidad establecidas en los numerales referentes a penas convencionales y deductivas por prestación deficiente del servicio y su cumplimiento normativo, así como el cálculo de las sanciones que resulten aplicables conforme a lo establecido en el Instrumento Contractual y la normatividad vigente; en este sentido, los reportes de administración deberán incluir dichos elementos.

- **Control presupuestario: KIO NETWORKS** con base en las solicitudes de servicio que se presenten durante la vigencia del contrato respectivo y la atención brindada a las mismas, incluyendo las cancelaciones correspondientes, realizará un informe analítico del importe de los servicios devengados que incluya un desglose por cada tipo de servicio en relación con los montos y máximos establecidos en dicho instrumento jurídico; lo anterior, a efecto de facilitar las actividades de verificación de los consumos presentados y tener un control presupuestario de los mismos. En este componente se incluirán también aquellos documentos impresos o electrónicos que incidan en este rubro tales como: tendencias en el consumo financiero, ejercicio presupuestal por dirección normativa, por aplicativo y por tipo de tecnología, esto es detallado por centro de costos, servicios devengados, control de saldos presupuestales (pasivos) y proyecciones presupuestales, entre otros.

- **Aspectos técnicos y metodológicos de los entregables: KIO NETWORKS** identificará y relacionará los elementos especificados en el contrato y sus anexos conforme a los cuales deberán presentarse los servicios considerando los entregables pactados, desde una perspectiva técnica y metodológica. Conforme a lo anterior, se incluirá en los reportes un informe que contenga los elementos exigidos en el contrato y sus anexos, con los cuales deberá acreditarse la entrega o prestación de los servicios.

Identificando, entre otros elementos: (i) forma; (ii) plazos, (iii) servidores públicos responsables de la recepción, sus cargos y ubicaciones; (iv) lugares de entrega o prestación de servicios; (v) procedimiento para la suscripción de las actas; (vi) documentación de soporte solicitada que acredite fehacientemente la entrega de los servicios devengados de conformidad con la funcionalidad solicitada así como los niveles de servicio establecidos, y en su caso la propuesta de la posible aplicación de penas convencionales y deductivas, entre otros elementos.

- **Esquema de integración de pagos: KIO NETWORKS** incluirá en los reportes la identificación de los elementos justificativos y comprobatorios que soporten la prestación de servicios durante el periodo que se reporte, conforme a las disposiciones normativas vigentes. Con esta información, **KIO NETWORKS** integrará la carpeta que soporte la solicitud de pago ante el **IMSS** por la entrega o prestación de los servicios devengados en el periodo mensual correspondiente, para su trámite y gestión por parte del Administrador del contrato, en términos de las facultades con que cuenta para la aceptación de los servicios.

- **Proyección del consumo de los servicios:** Con base en las facturas identificadas para pago, **KIO NETWORKS** elaborará un modelo gráfico y analítico que registre el consumo mensual real de cada uno de los servicios facturados y que permita un análisis comparativo respecto al consumo programado, a efecto de brindar al administrador del contrato información para la toma de decisiones.

Los reportes de administración para la gestión del conocimiento administrativo de los servicios deberán formar parte invariablemente de los documentos justificativos que soportan cualquier pago que se realice durante la vigencia del contrato correspondiente.

operación y administración del contrato, las cuales serán evaluadas por el IMSS y en su caso, autorizadas con o sin modificaciones, para su implementación y operación gradual o inmediata.

Para la exposición y análisis de la información presentada por **KIO NETWORKS**, habilitaremos al menos 3 pantallas de al menos 75 pulgadas, con todo lo necesario para la presentación de información de la operación de los servicios tecnológicos que permitan exponer de manera gráfica y ágil lo descrito en los dos párrafos anteriores, lo que permitirá contar con información en línea constante de la operación de los servicios contratados incluyendo elementos de análisis y detalles de la operación (parámetros de utilización) de la infraestructura ofertada además de la prestación de los servicios, además de indicadores de negocio que puedan ser descritos desde el alcance de cada contrato.

8.3 CLÁUSULAS Y CUMPLIMIENTO

8.3.1 Contrato de confidencialidad

KIO NETWORKS firmará un Contrato de confidencialidad mediante el cual **KIO NETWORKS** se obliga a no revelar, transferir, compartir ni ceder ningún dato o información de carácter sensible y confidencial que se hayan compartido entre **KIO NETWORKS** y el **IMSS**.

8.3.2 Cláusula de Opción para Obtención de Bienes al cierre de contrato (entregable de infraestructura)

Durante el último mes de la prestación del servicio, en caso de que el Instituto haya optado por la opción de compra, **KIO NETWORKS** realizará el proceso de entrega del equipamiento sujeto a la opción de compra por parte del Instituto. **KIO NETWORKS** se sujetará al procedimiento que el **IMSS** requiera para formalizar este proceso.

8.3.3 Documentación de cumplimiento de obligaciones

KIO NETWORKS con el objeto de fortalecer la supervisión y vigilancia de la administración del contrato materia del presente servicio y contribuir a las acciones para verificar la procedencia de los pagos, proporcionará un soporte especializado para la gestión del conocimiento administrativo relacionado con la prestación de los servicios de Nube **IMSS**.

Para que dicho conocimiento administrativo sea traducido en un activo del **IMSS**, **KIO NETWORKS** aplicará el modelo de control de contratos definido por el Grupo de Gobierno del Contrato y ejecutará las acciones que se establecen en dicho modelo como un ejercicio permanente durante la vigencia del contrato. Para tal efecto, se implementará un mecanismo para que dicho soporte especializado encargado de la gestión del conocimiento administrativo de los servicios objeto del presente anexo, cuente oportunamente con cada una de las solicitudes de servicio que se generen en el marco del contrato respectivo, así como respecto de todos los comunicados y documentos existentes entre el **IMSS** y **KIO NETWORKS** en relación con la prestación de los servicios. Lo anterior, toda vez que los servicios de soporte especializados previstos en ese aparatado están sujetos a flujo de información antes citada.

Lo anterior, con el fin de que **KIO NETWORKS** elabore los "Reportes de Administración" con corte mensual, que concluya las acciones relacionadas a la facturación presentada durante el periodo de la prestación del servicio, cuyo contenido se señala a continuación:

- **Gestión de los servicios:** Con base en las solicitudes u órdenes de servicio que genere el **IMSS**, **KIO NETWORKS** incluirá un desglose detallado del trámite que corresponde a la atención de cada una de ellas, en cuanto a su procedencia, tiempos límite de respuestas y demás circunstancias que se encuentren establecidas en el contrato respectivo y que permitan al Administrador del mismo tener control sobre dicha gestión, así como la documentación probatoria del devengo de los servicios, incluyendo toda la documentación o archivos electrónicos que demuestren la prestación del servicio, de conformidad a la funcionalidad solicitada y acorde a los niveles de servicio establecidos, siendo posible entre otros: reportes de monitoreo, disponibilidad, capacidad, desempeño y atención de incidentes, tickets de la mesa, actualizaciones, bitácoras, logs de aplicaciones, entre otros. En caso de que **KIO NETWORKS** no cuenta con la documentación probatoria de los servicios devengados, estos no podrán ser facturados.

- **Plataforma de obligaciones:** En este apartado, **KIO NETWORKS** elaborará un listado que identifique la totalidad de las obligaciones que se encuentran plasmadas en el contrato y sus respectivos anexos relacionados con los servicios. Asimismo, llevará a cabo su clasificación en atención a su importancia y consecuencia en:

  a) Obligaciones principales. Condicionantes del pago y los que están asociados a penas y deductivas
  b) Obligaciones secundarias. No condicionan el pago de los servicios, sin embargo, su cumplimiento es obligatorio en términos del instrumento contractual.

KIO NETWORKS presentará la documentación descrita en el presente punto, previo a solicitar el pago de sus servicios.

ANEXOS

DIVISIÓN DE CONTRATOS

KIO NETWORKS se presentará al Instituto, a través de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional cita en Av. Paseo de la Reforma No. 476, Anexo de Telecomunicaciones, Planta Alta, Col. Juárez, C.P. 06600, Ciudad de México, en un plazo no mayor a 5 (cinco) días hábiles posteriores a la adjudicación del contrato, al personal responsable del proyecto; en caso de que no se presente el personal en el plazo marcado, se aplicará la pena correspondiente.

KIO NETWORKS presentará en un plazo no mayor a 15 (quince) días hábiles posteriores a la adjudicación del contrato, un plan de trabajo general, para llevar a cabo la implementación del proyecto, en el que se especifiquen las actividades a realizar, la secuencia, los recursos asignados y responsables de dichas actividades, así como la duración del proyecto, su fecha de inicio y de conclusión marcando las fechas de entregables como son cantidad de servicios a entregar de forma única, mensual o eventual.

KIO NETWORKS entregará en un plazo no mayor a 15 (quince) días hábiles posteriores a la adjudicación del contrato, una matriz de escalación con el personal que gestionará los servicios de TIC y con los que el Instituto estará colaborando, su cargo y puesto, así como los datos y la vía de comunicación para contactarlo.

8 CONDICIONES TÉCNICAS DE ACEPTACIÓN DE ENTREGABLES

8.1 NORMATIVIDAD

Los entregables deberán cumplir con los lineamientos y procesos que indica el **MAAGTIC-SI** o la normatividad vigente durante la ejecución del contrato.

8.2 CUMPLIMIENTO DE OBLIGACIONES CONTRACTUALES

Para la documentación de Cumplimiento de Obligaciones contractuales, que permita una fácil y organizada atención de procesos de auditoria por parte de los entes de fiscalización, **KIO NETWORKS** elaborará en un plazo no mayor a 15 (quince) días hábiles posteriores a la adjudicación del contrato, una matriz de los verbos, pronombres, tiempos y compromisos presentes en el anexo técnico, términos y condiciones, apéndices o documentación complementaria al anexo, así como en la propia oferta de **KIO NETWORKS**, a fin de contar con un listado de todos los verbos de acción, conjunciones, excepciones, interacciones, consideraciones de tipo y frecuencia de información electrónica que deba incluirse, casos de uso y en su caso especificaciones o excepciones, para convertirlos en los "documentos probatorios de cada obligación establecida en el contrato".

A partir de este listado, de manera conjunta entre el **IMSS** y **KIO NETWORKS**, en un plazo no mayor a 10 (diez) días hábiles posteriores a la entrega del listado por parte de **KIO NETWORKS** cuando resulte adjudicado, generará el detalle de los documentos tanto en formato, contenido, información adjunta en imágenes, archivos o documentos complementarios, así como firmas y validaciones a efectuarse por el personal que participará en los procesos de entrega de servicios, lo cual se depositará en un repositorio documental que habilitará **KIO NETWORKS** con acceso permanente a los administradores del contrato (cuerpo de gobierno del contrato), los cuales analizarán al menos quincenalmente con el gerente de cuenta y personal técnico por parte de **KIO NETWORKS**, el avance de los proyectos, la continuidad operativa, siguientes compromisos y la documentación del ejercicio del gasto y cumplimiento de niveles de servicio establecidos, siendo parte fundamental la documentación de Cumplimiento de Obligaciones contractuales, incluyendo en su caso, las penas convencionales o deductivas aplicables. En estas juntas de gobierno del contrato, **KIO NETWORKS** debe exponer al personal IMSS, los detalles de la operación, consumos, tendencias, áreas de oportunidad y mejores prácticas susceptibles de incorporarse a la

6 ESPECIFICACIONES TÉCNICAS

Las especificaciones técnicas referentes a este apartado del anexo técnico se encuentran detalladas en el apartado **CARACTERÍSTICAS DE LOS SERVICIOS.**

7 PERFIL DE KIO NETWORKS

KIO NETWORKS acredita ser una empresa con la capacidad y experiencia técnica requerida para proporcionar el servicio solicitado, anexando currículo de la misma.

KIO NETWORKS entrega al Instituto "La Opinión del Cumplimiento de Obligaciones en materia de Seguridad Social" vigente y positiva. Asimismo, **KIO NETWORKS** queda obligado a entregar al Instituto junto con la factura de cobro respectiva, la "Opinión del Cumplimiento de Obligaciones en materia de Seguridad Social" vigente y positiva.

KIO NETWORKS entrega el documento vigente expedido por el SAT en el que se emita la opinión de cumplimiento de las obligaciones fiscales, positivo y vigente.

KIO NETWORKS cuenta con experiencia comprobable para brindar los servicios objeto de la presente Propuesta Técnica, apéndices, así como términos y condiciones.

Certificaciones enunciativas más no limitativas en:

- CCIE Routing and Switching
- CCDP Diseño Profesional de redes.
- ITIL Foundation Certificate in IT Service Management
- Symantec Data Loss Prevention Prevention 14.5
- Symantec Messaging Gateway
- ISO/IEC 27001
- ISO/IEC 20000
- ITIL intermediate in Operational support and analysis
- ITIL intermediate in Service Offering AND Agreements
- ITIL intermediate un Release, control and validation.
- PCNSE Network Security Engineer 7
- MCITP Enterprise Administrator on Windows Server 2008
- MCTS Microsoft Exchange Server 2007 Configuration
- Enterasys Certified Specialist – Routing
- Certificación ITIL RCV, 2017
- Certificación ITIL SOA, 2016
- Certificación ITIL OSA, 2012
- PMI

KIO NETWORKS cuenta con el personal certificado en Metodologías de Administración de Proyectos para la dirección del proyecto.

ANEXOS

DIVISIÓN DE CONTRATOS

los entregables de única ocasión de acuerdo al ***plan de entrega*** establecido en conjunto con el **IMSS**. La validación de cada servicio será supervisada por personal que el **IMSS** designe.

5.3 LICENCIAMIENTO

La solución ofertada por **KIO NETWORKS** considerará la totalidad de licencias de la solución integral para brindar todos los requerimientos establecidos en el presente anexo. La vigencia del licenciamiento para todos los servicios es necesaria desde su instalación durante la vigencia del contrato. En caso de que el **IMSS** requiera de licenciamiento adicional para el correcto funcionamiento de todos sus componentes este será proporcionado por **KIO NETWORKS** como parte del servicio.

5.4 PROCESOS

KIO NETWORKS entregará toda la documentación que se genere durante la vigencia del contrato y estará apegada a los formatos y procesos de **MAAGTIC-SI** o la normatividad vigente durante la ejecución del contrato. Los formatos que solicita el **IMSS** referentes al **MAAGTIC-SI** son los que actualmente están vigentes, sin embargo, al momento de la contratación y durante la vigencia del contrato dichos formatos solicitados en el presente anexo técnico podrán actualizarse, cancelarse, modificarse, sustituirse y/o en su caso incrementarse los formatos de acuerdo a los lineamientos que establezca la **Secretaría de la Función Pública** y la normatividad vigente.

5.5 RECURSOS HUMANOS

KIO NETWORKS incluye los Recursos Humanos necesarios para la implantación y puesta en marcha de los servicios descritos en el presente anexo técnico, de acuerdo a los tiempos y niveles de servicio establecidos. El personal que realice funciones de coordinación, supervisión o cualquier otra función similar o superior que **KIO NETWORKS** proporcione, tendrá el enfoque de atención a clientes, servicio y conocimiento técnico y operativo.

En caso de existir algún inconveniente con el personal, éste será reemplazado en caso de que el área lo solicite. Este cambio deberá realizarse en un plazo no mayor a 10 días hábiles.

Contará con personal calificado y certificado de segundo y tercer nivel para atender los incidentes presentados en los servicios, para lo cual deberá trasladarse a las instalaciones del **IMSS** las veces que sea necesario.

Es importante señalar que, en base a las necesidades de las Unidades Responsables del **IMSS**, esta lista podrá ser modificada de tal manera que pueda solicitarse la rotación de personal o el movimiento temporal de los técnicos especialistas para atender eventos que así lo requieran.

KIO NETWORKS considera que el **IMSS** podrá requerir el apoyo de los ingenieros fuera de los días y horario mencionado para la atención del *Servicio* (Por eventos especiales, reubicaciones, servicios temporales, etc.), por lo que este tipo de solicitudes estarán consideradas por **KIO NETWORKS**.

Deberá existir personal en un esquema 7x24, en caso de que el Instituto requiera alguna eventualidad, se notificara para la coordinación respectiva con **KIO NETWORKS** por lo que estarán disponibles para la atención.

5.6 CLÁUSULA DE OPCIÓN PARA LA OBTENCIÓN DE BIENES AL CIERRA DEL CONTRATO

El último mes de la prestación del servicio, el **IMSS** podrá evaluar quedarse con los bienes o conservar los bienes para lo cual informará a **KIO NETWORKS** su decisión sobre la opción de compra de los bienes que integran el proyecto, **KIO NETWORKS** presentará propuesta económica del o los componentes de hardware/software que integran cada uno de los servicios descritos en el presente anexo técnico, así como sujetarse al procedimiento que establezca el **IMSS** para formalizar este proceso.

Durante el último mes de la prestación del servicio, en caso de que el Instituto haya optado por la opción de compra, **KIO NETWORKS** realizará el proceso de entrega del equipamiento sujeto a la opción de compra por parte del Instituto. **KIO NETWORKS** se sujetará al procedimiento que el **IMSS** requiera para formalizar este proceso.

4.6.3.5 Consideraciones generales para la entrega de servicios extendidos

A continuación, se señalan de manera enunciativa, más no limitativa, los proyectos y servicios que el Instituto identifica como de soporte extendido, entendiendo que dichos servicios pueden o no ser requeridos a través del Grupo de Gobierno del Contrato, durante la vida del contrato, sin menoscabo de que sean requeridos cualquier otro proyecto o servicio relacionado con los servicios administrados descritos en el presente Anexo Técnico:

- Servicios especializados de arquitectura, administración y soporte técnico no previstos en el Anexo Técnico con motivo de nuevos requerimientos y/o nuevas tecnologías requeridas por el Instituto relacionados al objeto de la presente Propuesta Técnica.
- Servicios de Análisis de integración de proyectos y/o servicios pertenecientes a nuevos dominios tecnológicos requeridos para la continuidad de los servicios considerados en el presente Anexo Técnico.

Servicios específicos de apoyo al Grupo de Gobierno de Contrato en relación a nuevos procesos, herramientas o mecanismos de operación y control no definidos en este Anexo Técnico y que sean necesarios para mejorar el desempeño de los servicios del contrato.

5 PLAN DE ASEGURAMIENTO DE LA CALIDAD

5.1 CONDICIONES GENERALES

KIO NETWORKS proveerá de los insumos y equipos necesarios para ofrecer el servicio. Los incidentes y solicitudes deberán gestionarse para su atención a través de una mesa de servicios o centro de operaciones de **KIO NETWORKS.** Todo el servicio técnico preventivo, correctivo, así como partes, refacciones y consumibles serán incluidos como parte del servicio.

KIO NETWORKS ejecutará las acciones que permitan tener la calidad necesaria y garantizar la confidencialidad, integridad y disponibilidad requerida de los servicios que se describen en el presente anexo.

KIO NETWORKS monitoreará el estado de los equipos y servicios de tal manera que se generen acciones proactivas para corregir fallas sobre procesamiento, almacenamiento, red de telecomunicaciones, seguridad y servicios de voz, de la cual se proporciona la arquitectura actual.

KIO NETWORKS cuenta con experiencia comprobable en la implementación y puesta a punto de servicios especificados en el presente anexo que garanticen la continuidad de los servicios del Instituto; y certificaciones tanto de la infraestructura y el personal de **KIO NETWORKS** en las tecnologías ofertadas. Así mismo, demostrar mediante contratos similares (al menos 3) mediante una copia legible de contratos, pedidos y/o cartas del cumplimiento de proyectos de la misma naturaleza.

KIO NETWORKS incluye un administrador de proyectos certificado en Project Manager Professional (PMP) por el Project Management Institute (PMI). Así mismo presentará su certificación vigente durante la vigencia del contrato.

El centro de datos **ofertado por KIO NETWORKS** estará certificado por el UPTIME INSTITUTE con el nivel de TIER III, el cual se utilizará para hospedar el equipamiento especificado en los servicios de aprovisionamiento.

5.2 ACEPTACIÓN DEL SERVICIO

La aceptación del servicio se dará cuando el **IMSS** valide por cada plataforma tecnológica lo siguiente:

Se dará por aceptado el servicio cuando todos los componentes y servicios que lo integran estén **instalados, configurados, puesta en marcha de la solución** y **validados por el personal asignado del IMSS**, de acuerdo a lo establecido en este anexo y se realice entrega de los documentos comprobatorios relacionados a cada servicio de la presente Propuesta Técnica, así como se cumpla con

ANEXOS
DIVISIÓN DE CONTRATOS

- Para las Unidades de Soporte Extendido para el **Servicio de Seguridad** será del 5% del costo unitario mensual del servicio.
- Para las Unidades de Soporte Extendido para **el Servicio de Continuidad de la Operación y Soporte** será del 5% del costo unitario mensual del servicio.

Los servicios que estarán a cargo de **KIO NETWORKS** para cada una de las Unidades de Soporte Extendido serán los necesarios para cumplir con los objetivos y alcance del Proyecto-Servicio.

4.6.3.2 Requisitos del Servicio

Los servicios o proyectos solicitados a través de esta modalidad tienen carácter de finitos en el tiempo y serán correctamente acotados en alcance conforme a la documentación que se señala a continuación. Para cada solicitud de Proyecto-Servicio que efectúe el Instituto a través de un Administrador del Contrato Respectivo, **KIO NETWORKS** será responsable de definir al menos, por escrito, con papel membretado de su empresa y firmado por el Representante Legal de la misma, los siguientes elementos con lujo de detalle:

1. Objetivos del Proyecto-Servicio
2. Alcances del Proyecto-Servicio
3. Actividades a realizar (Plan de Trabajo Detallado) que incluya fechas compromiso para los distintos entregables
4. Desglose técnico de los componentes que integren el servicio a prestar
5. Memoria técnica de los servicios (Información anexa de soporte, documentación y apoyo)
6. Justificación técnica de la correspondencia del objetivo del proyecto o servicio con las Unidades de Soporte Extendido de conformidad con el alcance técnico del mismo.

El costo unitario de estos servicios se deriva de la propuesta económica de **KIO NETWORKS**. Estos servicios no forman parte de la propuesta económica y son adicionales dentro del monto máximo del contrato que resulte del presente proceso. **KIO NETWORKS** incluirá en su propuesta técnica la afirmación de prestar en los términos descritos.

4.6.3.3 Mecanismo de consumo de las Unidades de Soporte Extendido

A continuación, se muestran ejemplos de manera enunciativa más no limitativa y como referencia de los Proyectos-Servicios posibles a solicitar con las Unidades de Soporte Extendido de conformidad a la justificación técnica evaluada entre **KIO NETWORKS** y el Instituto, los siguientes:

a) Análisis de incorporación de servicios no previstos en esta Propuesta Técnica

b) Análisis de integración de servicios de comunicaciones, voz, video o datos pertenecientes a dominios ajenos a los servicios de la presente Propuesta Técnica.
c) Labores específicas de apoyo al Instituto y al GGC en procesos no definidos en esta Propuesta Técnica.
d) Consultoría de descubrimiento y documentación detallada de estado actual de otros servicios de tecnologías de información y comunicaciones (TIC), así como de servicios de datos, voz, imagen, comunicaciones unificadas, video y otros relacionados.
e) Trabajos tendientes a la homogenización de servicios TIC, dentro de los cuales pudiera incluirse la provisión de servicios administrados.
f) Análisis y definición técnica de casos de uso de negocio para la interpretación de tráfico, de datos, de servicios digitales y electrónicos bajo la administración del IMSS.

4.6.3.4 Modalidad de Soporte Extendido

Cada servicio deberá recibir un tratamiento individual por parte de **KIO NETWORKS**, para lo cual designará a un **Coordinador de Proyecto de Soporte Extendido** por solicitud, quien será responsable del seguimiento y control de la solicitud hasta su finalización. Dicho coordinador deberá asistir a las reuniones requeridas por el Instituto para determinar el alcance del proyecto, así como dar el seguimiento al mismo hasta su conclusión.

Todo el personal designado por **KIO NETWORKS** para atender un proyecto o servicio de soporte extendido, no podrá pertenecer a los grupos que brindan cualquiera de los servicios descritos en el resto de los apartados de la presente Propuesta Técnica (salvo que se demuestre que es indispensable para el proyecto y en cuyo caso no deberán incluirse sus horas en la cotización, a menos que se demuestre que será reemplazado por alguien más en las funciones que generalmente realiza, sin menoscabo o riesgo del servicio en el que participa); y deberán contar con certificación o experiencia equivalente y comprobable para la prestación de los servicios a los que sean asignados, siendo en todo momento prerrogativa del Instituto la aceptación previo al inicio del servicio, de la persona y/o grupo de trabajo que participan, reservándose el derecho de solicitar el cambio del personal o recursos asignados al proyecto.

- Middleware
- Automatización y gestión de procesos
- Productividad
- Controles de seguridad
- Comunicación unificada y colaboración
- Visualización
- Acceso Web

El dominio de Infraestructura tiene por objeto proporcionar un esquema de categorización para los activos físicos de TI, los sistemas operativos y firmware que los controlan, y los lugares o instalaciones que albergan los activos de TI físicos. Se divide en tres áreas, Plataforma, Red e Instalaciones, que están vinculados y relacionados entre sí para permitir el análisis de los activos de TI a través de las tres dimensiones.

- La plataforma incluye la arquitectura de hardware y el marco de trabajo para el software, donde la combinación permite que el software pueda ejecutarse, en particular software de aplicación. Las plataformas incluyen la arquitectura de computadoras, el sistema operativo y los dispositivos internos; así como plataformas de software que emulan las plataformas de hardware completas (por ejemplo, la virtualización del sistema); y se incluyen las siguientes categorías, a manera de referencia:
  - Hardware
  - Sistema operativo
  - Hardware de telecomunicaciones
  - Dispositivos periféricos
  - Virtualización
  - Nodo de Extensión de Nube Privada (ENP)
- La red describe los Bloques de Construcción Fundamentales que permiten acceder a un BCF o BCC en particular, utilizado dentro de los servicios de la presente Propuesta Técnica; y se incluyen las siguientes categorías, a manera de referencia:
  - Zona
  - Tipo de red
  - Infraestructura
  - Tipo de transmisión
- Las instalaciones proporcionan el esquema de categorización para describir cómo y/o donde un BCF o BCC determinado será instalado, desplegado, y operado (para efectos de esta Propuesta Técnica, se corresponden con las modalidades de despliegue mencionadas anteriormente); y se incluyen las siguientes categorías, a manera de referencia:
  - Nodos de Extensión de Nube Privada (ENP)
  - Ambientes no productivos
  - Centro de Datos externo (Centro de Datos Primario)
  - Nodos de Extensión de la Nube Híbrida (ENH) del IMSS
  - Instalaciones designadas por el Instituto

Los BCF, sus características, versiones y especificaciones técnicas se encuentran dentro del Apéndice "1.Bloques de Construcción". Es importante señalar que tales BCF serán proporcionados como Servicios

Administrados por lo que deberán contar de manera integral con todos los servicios de Soporte y Operación asociados a los mismos conforme a lo especificado en el presente Anexo Técnico.

4.6.2 Servicio de Plataformas y Bloques de Construcción Comunes.

4.6.2.1 Bloques de Construcción Comunes

Un Bloque de Construcción Común representa un grupo de componentes que son relevantes tecnológica y operativamente en su conjunto para una o más soluciones para el Instituto. Incluyen colecciones de capacidades y requerimientos comunes a diferencia de aquellos particulares de los de una solución específica, proveen estructuras con ambientes operativos específicos para las necesidades operativas y de información en la construcción de soluciones de negocio particulares.

Por solicitud del Instituto se declararán Bloques de Construcción Común definidos entre el Instituto y **KIO NETWORKS**. Una vez declarados los Bloques de Construcción Común, se tendrá un precio por BCC y en lo sucesivo se devengará por BCC y no por BCF. Así mismo, los niveles de servicio serán medidos por BCC y no por BCF por lo que las penas convencionales y deductivas que apliquen serán aplicadas al BCC.

KIO NETWORKS en conjunto con el Instituto definirá un tiempo máximo para la habilitación de BCFs como BCC. En caso de que **KIO NETWORKS** no habilite el BCC en el plazo acordado, aplicarán las penas convencionales generales que establece el presente Anexo Técnico.

4.6.3 Servicios Extendidos de Soporte

El servicio de Soporte Extendido se contratará bajo demanda y se ejercerá a partir de las Unidades de Soporte Extendido, cada solicitud de proyecto recibirá un tratamiento individual por parte de **KIO NETWORKS**.

4.6.3.1 Descripción del Servicio

El costo unitario de las Unidades de Soporte Extendido se calculará con base en la propuesta económica de **KIO NETWORKS**, en los términos siguientes:

- Para las Unidades de Soporte Extendido para el **Servicio de Soporte para la Integralidad y Telecomunicaciones** será del 5% del costo unitario mensual del servicio.

ANEXOS
DIVISIÓN DE CONTRATOS

4.5.3 De la fase de propuesta para su implementación en un estado mínimo funcional

- **KIO NETWORKS** incluye en su propuesta, que, considerando el resultado de la fase anterior, presentará una propuesta para la reducción del ecosistema del aplicativo o componente Institucional seleccionado.
- **KIO NETWORKS** hará una medición de los recursos, los servicios y los procesos mínimos necesarios, que permitan poner en operación el aplicativo o componente seleccionado por el Instituto, priorizando las características de eficiencia, eficacia y austeridad.
- En esta fase, **KIO NETWORKS** presentará los niveles de desempeño necesarios del aplicativo o componente en su versión mínima, previa validación por el Instituto.
- **KIO NETWORKS** documentará todas y cada una de las actividades realizadas; se dará por concluida esta fase, una vez que haya sido aceptado y firmado el entregable, conforme al alcance y actividades propuestas por **KIO NETWORKS** y autorizadas por el personal que el Instituto designe.
- **KIO NETWORKS** realizará un flujo de trabajo de su propuesta, considerando las relaciones e interdependencias del aplicativo o componente seleccionado con otros, propios del Instituto o relacionados con otras Instituciones y socios comerciales, llevará a cabo la presentación del flujo de trabajo y de la documentación de este, considerando los resultados y nuevos hallazgos o mejoras identificados durante su presentación.
- El servicio se solicitará y ejecutará bajo demanda, considerando las necesidades de cumplimiento con las autoridades correspondientes y necesidades del Instituto.
- **KIO NETWORKS** entregará el flujo de trabajo final que permita al Instituto la ejecución de las pruebas de laboratorio de medición del desempeño del aplicativo o componente seleccionado.

Entregables de esta fase:

- El entregable de esta fase consiste en un informe que incluya: la propuesta del flujo de trabajo detallada, para el aplicativo o componente Institucional en su versión mínima y completamente funcional; es decir, que permita cumplir con la naturaleza de su desarrollo y puesta en marcha.
- El informe deberá integrar una metodología y su respectivo plan de trabajo general, que permita al Instituto y en caso de ser requerido, la ejecución de las pruebas de laboratorio de medición del desempeño del aplicativo o componente seleccionado.
- **KIO NETWORKS** realizará la debida transferencia de conocimiento del flujo de trabajo para la ejecución de las pruebas del *Laboratorio de Medición del Desempeño en su versión mínima y funcional*, identificando la operación colaborativa con el personal designado por el Instituto, para la aplicación de la estrategia desarrollada e implementada, considerando en esta los cambios organizacionales cuando ocurran.

- **KIO NETWORKS** trabajará en conjunto con el Instituto para comunicar y entrenar a los servidores públicos relacionados con esta fase, acerca de sus roles y responsabilidades, para cumplir lo establecido en los objetivos de esta de acuerdo al plan de trabajo desarrollado.
- Finalmente, se dará por concluida esta fase, una vez que haya sido aceptado y firmado el entregable, conforme al alcance y actividades propuestas por **KIO NETWORKS** y autorizadas por el personal que el Instituto designe.

4.6 ELEMENTOS COMUNES DE LOS SERVICIOS

4.6.1 Servicio de Infraestructura y Bloques de Construcción Fundamentales

KIO NETWORKS aprovisionará cualquiera de los BCF establecidos en el apéndice "Bloques de Construcción" en la modalidad de Infraestructura como Servicio. En dicho apéndice se describen los distintos tipos de componentes considerados como BCF a los cuales el Instituto podrá tener acceso durante la vigencia del contrato.

El dominio de aplicaciones incluye dos áreas: sistemas y componentes de aplicaciones; los cuales vienen empaquetados y son autocontenidos y se refieren exclusivamente al software, por lo que se deben integrar con los BCFs de Infraestructura descritos más adelante.

- Los sistemas son conjuntos discretos de recursos de información, organizados para la recolección, procesamiento, mantenimiento, uso, distribución, difusión o disposición de información para sustentar un proceso de negocio específico del Instituto; y se incluyen las siguientes categorías, de manera enunciativa más no limitativa:
  - Sistemas de gestión de adquisiciones
  - Gestión financiera
  - Administración del personal
  - Gestión de recursos humanos
  - Gestión de activos y propiedades
  - Gestión de la seguridad
  - Gestión de los sistemas
- Los componentes de aplicación corresponden al software autocontenido mismo que podrá ser agregado o configurado para sustentar diferentes capacidades; y se incluyen las siguientes categorías, a manera de referencia:
  - Análisis, reporteo y estadísticas
  - Gestión de datos
  - Herramientas y entorno de desarrollo
  - Gestión de documentos y contenidos
  - Descubrimiento y gestión del conocimiento

4.5.1 De la fase de diagnóstico inicial del estado de aplicativos y componentes Institucionales

- **KIO NETWORKS** considerará la información con la que actualmente operan los aplicativos institucionales en el centro de datos tercerizado para cada aplicativo o componente que el Instituto determine. Este análisis será documentado con base en la infraestructura usada en la actualidad y considerando en todo momento lo siguiente: licenciamiento, servidores, manejadores de bases de datos, almacenamiento, telecomunicaciones y otros componentes de infraestructura que sean necesarios para la operación actual; así mismo las interdependencias con otros aplicativos, componentes transversales, propios del Instituto y externos.
- **KIO NETWORKS** realizará y proveerá de diagramas de arquitectura tecnológica detallados, la descripción precisa y las capacidades actuales de cada activo de información utilizado dentro de la infraestructura del centro de datos tercerizado, así mismo y hasta donde sea posible, de los componentes transversales utilizados en cada aplicativo y otras interdependencias.
- **KIO NETWORKS** generará los documentos y reportes requeridos por el Instituto con la intención de presentar avances y resultados de esta fase y las actividades asociadas.
- Es importante mencionar que **KIO NETWORKS** entregará un diagnóstico completo para que el Instituto tenga información detallada y que dé una visión completa acerca del estado actual de operación de los aplicativos o componentes seleccionados por el Instituto.

Entregables de esta fase:

- El entregable de esta fase consiste en un informe que incluya: el plan de trabajo, los diagramas de arquitectura tecnológica con todos los activos de información relacionados, su respectiva descripción, incluyendo el estado actual de capacidades tecnológicas y comportamiento del aplicativo o componente hasta donde sea posible.
- Además, **KIO NETWORKS** realizará la debida transferencia de conocimiento para la *Gestión de Medición del Desempeño*, identificando la operación colaborativa con el personal designado por el Instituto, para la aplicación de la estrategia desarrollada e implementada, considerando en esta los cambios organizacionales cuando ocurran.
- **KIO NETWORKS** trabajará en conjunto con el Instituto para comunicar y entrenar a los servidores públicos relacionados con esta fase, acerca de sus roles y responsabilidades, para cumplir lo establecido en los objetivos de esta, de acuerdo con los planes de trabajo desarrollados.
- Finalmente, se dará por concluida esta fase, una vez que haya sido aceptado y firmado el entregable, conforme al alcance y actividades propuestas por **KIO NETWORKS** y autorizadas por el personal que el Instituto designe.

4.5.2 De la fase de optimización del estado actual para mejora del desempeño óptimo:

- A partir del resultado de la fase anterior, **KIO NETWORKS** identificará y actualizará los cambios de o hacia los activos de información que componen la operación de los aplicativos o componentes Institucionales seleccionados, ubicados y utilizados en la infraestructura propiedad del Instituto, la del centro de datos tercerizado hasta donde sea posible y de sus socios comerciales.
- **KIO NETWORKS** hará una medición de capacidades actuales de: los recursos, los servicios y los procesos, que permitan aislar y optimizar la operación del aplicativo o componente seleccionado por el Instituto, priorizando las características de eficiencia y eficacia.
- En este análisis, **KIO NETWORKS** debe determinar los niveles de desempeño óptimo del aplicativo o componente comparado con el estado actual, previa validación por el personal designado por el Instituto.
- **KIO NETWORKS** documentará todas y cada una de las actividades realizadas; se dará por concluida esta fase, una vez que haya sido aceptado y firmado el entregable, conforme al alcance y actividades propuestas por **KIO NETWORKS** y autorizadas por el personal que el Instituto designe.
-

Entregables de esta fase:

- El entregable de esta fase consiste en un informe que incluya: la mejora del aplicativo o componente seleccionado considerando las características de eficiencia y eficacia, justificando minuciosamente las mejoras propuestas y realizando un comparativo del estado actual con esta.
- Además, **KIO NETWORKS** incluye en su propuesta que realizará la debida transferencia de conocimiento para la *Medición del Desempeño Óptimo*, identificando la operación colaborativa con el personal designado por el Instituto, para la aplicación de la estrategia desarrollada e implementada, considerando en esta los cambios organizacionales cuando ocurran.
- **KIO NETWORKS** incluye en su propuesta que trabajará en conjunto con el personal del Instituto para comunicar y entrenar a los servidores públicos relacionados con esta fase, acerca de sus roles y responsabilidades, para cumplir lo establecido en los objetivos de esta, de acuerdo con el plan de trabajo desarrollado.
- Finalmente, se dará por concluida esta fase, una vez que haya sido aceptado y firmado el entregable, conforme al alcance y actividades propuestas por **KIO NETWORKS** y autorizadas por el personal que el Instituto designe.

ANEXOS

DIVISIÓN DE CONTRATOS

concurrentes, entre otros, conforme la naturaleza y características del servicio que dicha infraestructura y base instalada soportan.

Integrar a los servicios de gestión, operación, soporte y mantenimiento provistos por su Centro de Operaciones de Seguridad (SOC) para los servicios ofrecidos, dando cumplimiento a las condiciones del presente contrato.

Establecer Mesas de trabajo con el Instituto, a fin de llevar a cabo la planeación para la toma de operación de la infraestructura y base instalada, con el propósito de no afectar la continuidad operativa, de negocios o de seguridad de este último.

Poner en marcha los servicios de su Centro de Operaciones de Seguridad (SOC), así como establecer los enlaces de comunicaciones que los interconecten con la red de Gestión del Instituto previo a la transición a la operación del servicio.

Establecer su Mesa de Servicio, para lo cual, durante la fase de toma de operación y transición, tendrá ya disponible un servicio de Mesa de Servicio.

Proporcionar la información relacionada con la documentación que soportan los servicios, incluyendo entre otros, memorias técnicas, manuales y/o procedimientos de atención de servicios, matrices de escalamiento que permitirán al Instituto validar en cualquier momento los elementos que componen los diversos servicios.

4.4.3 Consumo de BCFs y BCCs para el servicio de seguridad

El SSNI podrán consumir BCFs y BCCs que se encuentren disponibles según lo que se describe en este mismo apartado "Servicio de Operación y Calidad de la Seguridad Informática Perimetral" para todas las modalidades de despliegue, conforme a lo que se especifica en la sección "3.6 Elementos comunes de los Servicios", será responsable de validar su consumo y disponibilidad valiéndose de la información de que proporcionen sus propios servicios de "Soporte para la Calidad de la Seguridad de la Nube IMSS" y "Soporte para la Operación de la Seguridad de la Nube IMSS".

4.4.4 Servicios eventuales de seguridad

A lo largo del servicio de Soporte para la Calidad de la Seguridad de la Nube IMSS y de Soporte para la Operación de la Seguridad de la Nube IMSS, se señalan una serie de servicios que pueden ser consumidos de manera eventual. Dichos servicios serán cotizados de manera individual según se señala en la sección Catálogo de Servicios.

4.4.5 Servicios extendidos

Conforme a lo señalado en la sección Elementos comunes de los Servicios, los servicios extendidos se derivan del servicio de Soporte para la Calidad de la Seguridad de la Nube IMSS y del servicio de Soporte para la Operación de la Seguridad de la Nube IMSS.

4.5 Servicio de Gestión de Medición del Desempeño de Aplicativos y Componentes Institucionales

KIO NETWORKS incluye en su propuesta que proporcionará al Instituto el servicio descrito en la presente sección, para el cual se deberán incluir las siguientes fases: a) diagnóstico inicial del estado de aplicativos y componentes institucionales, b) optimización del estado actual para mejora del desempeño óptimo y, c) propuesta para su implementación en un estado mínimo funcional. A partir del desarrollo de las fases antes indicadas, el Instituto determinará y notificará a **KIO NETWORKS** si es requerido probar las fases antes descritas, considerando para ello, la infraestructura que el Instituto determine.

KIO NETWORKS incluye en su propuesta que se apegará al marco tecnológico de referencia y a los lineamientos Institucionales establecidos para aplicativos, software, componentes, infraestructura, telecomunicaciones y seguridad, para la entrega de componentes, servicios e infraestructura que permitan efectuar las pruebas de medición de desempeño en el Centro de Datos Institucional o en otro Centro de Datos que el Instituto designe para tal efecto.

Así mismo, **KIO NETWORKS** se apegará al marco tecnológico de referencia y a los lineamientos Institucionales establecidos para aplicativos, software, componentes, infraestructura, telecomunicaciones y seguridad, para la entrega de componentes, servicios e infraestructura que permitan efectuar las pruebas de medición de desempeño en el Centro de Datos de **KIO NETWORKS** que resulte adjudicado o en otro Centro de Datos que el Instituto designe para las pruebas.

KIO NETWORKS incluye en su propuesta la posibilidad de atención bajo demanda por parte del Instituto, que realizará el análisis y desarrollo solicitado para atender requerimientos de Nivel Central y en caso de así solicitarlo en Instituto, de las 35 oficinas de representación institucional, permitiendo al Instituto el cumplimiento de objetivos, metas y diferentes requerimientos por parte de entidades fiscalizadoras cuando así lo soliciten.

KIO NETWORKS ofrece, detallar y describir en su propuesta que el servicio requerido por el Instituto incluirá por lo menos los siguientes elementos:

- Archivos electrónicos (MS Excel) con la información fuente obtenida de las herramientas tecnológicas que se utilizaron para realizar las pruebas de penetración.
- Reporte de las pruebas de penetración realizadas, indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de ejecución, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja).

4.4.2.4.1.3 Análisis Forenses

Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle del análisis forense ejecutado por cada activo o grupo de activos de infraestructura verificados.

4.4.2.4.1.4 Borrado Seguro de Datos

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro por cada activo o grupo de activos de infraestructura eliminados.
- Archivos electrónicos (Html y PDF) con la información fuente obtenida de las herramientas tecnológicas que se utilizaron para realizar los borrados seguros de la información.
- Reporte mensual de los borrados seguros realizados, indicando al menos: Activo(s) de infraestructura, fecha de eliminación.

4.4.2.4.1.5 Análisis de Riesgos de Seguridad de la Información

- Reporte ejecutivo en formato electrónico (MS Word, PDF) de la actividad de Análisis de Riesgos que incluya:
  - Identificación activos, considerando como activos a los procesos, actividades, información, infraestructura, y gente.
  - Identificación de vulnerabilidades.
  - Identificación de amenazas.
  - Escenarios de riesgo.
  - Priorización del riesgo.

4.4.2.4.1.6 Sistema de Gestión de Seguridad de la Información (SGSI)

- Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora del Sistemas De Gestión de Seguridad de la Información que incluya:
  - Capacitación inicial
  - Generación de directivas de seguridad
  - Identificación y valuación de activos
  - Generación de la Declaración de Aplicabilidad
  - Generación del plan de tratamiento de riesgos
  - Propuestas de implementación de los controles
  - Manual de Gestión de Seguridad de la Información

Los reportes y/o documentos anteriores serán entregados en el formato y fecha que hayan sido acordados con el órgano de gobierno del Instituto que los haya solicitado; y serán integrados al **Entregable Mensual del Servicio de Seguridad)** en el periodo que corresponda a su entrega, para la validación de los niveles de servicio que correspondan.

4.4.2.5 Consideraciones generales para la entrega de los servicios de seguridad

KIO NETWORKS cumplirá con:

Fortalecer la seguridad de la información de la Institución contra amenazas, disminuyendo el riesgo de sufrir incidentes de seguridad, mediante el uso de tecnología de punta para el monitoreo, detección, aseguramiento, y contención de ataques que puedan presentarse en la infraestructura de cómputo, sistemas y aplicaciones del Instituto.

Contar con servicios de infraestructura regulados por niveles de servicio, que: implementen (instalen, migren, habiliten y pongan a punto) los componentes necesario en los Centros de Datos del Instituto, u otras localidades que este último designe, y que de forma complementaria gestionen (operen, monitoreen, den soporte y mantenimiento preventivo y correctivo) a la correspondiente infraestructura con el propósito de satisfacer las necesidades de: conectividad, comunicación, protección, control y filtrado de la propia Institución, manteniendo la plataforma tecnológica en condiciones óptimas de operación.

Contar con los servicios de protección de forma unificada e integrada, incluyendo protección de servidores, conectividad, navegación, filtrado, entre otros; mediante una solución integral que permita una gestión consolidada de las funcionalidades, características y servicios, con el propósito de mantener y robustecer el esquema de seguridad del Instituto.

Contar con servicios de seguridad de la información, que complementen el esquema de seguridad Institucional de forma consistente y robusta, con el control, aseguramiento, diagnóstico, protección, pruebas, metodologías, de distintos rubros como el de acceso a cuentas privilegiadas, base de datos, aplicaciones, fuentes múltiples, vulnerabilidades, investigación forense y de procesos de seguridad, así como con otros servicios especializados en materia de seguridad y tecnologías de la información.

Efectuar la actualización de cualquier tipo de licencia, componente, dispositivo, parche, arquitectura, etc. siempre y cuando el fabricante de dicho componente haya liberado una versión que lo reemplace por aspectos de seguridad, compatibilidad, error o falla detectada, o similar; con la finalidad de mantener estable y segura la operación de los servicios del Instituto, entendiendo que toda actualización o mejora debe ser consultada y aprobada por este último.

Garantizar la operación, licenciamiento, soporte técnico, mantenimiento correctivo y preventivo, así como el reemplazo de partes (por parte del fabricante del componente o de la solución), de los servicios propuestos, considerando la cantidad de unidades de licenciamiento como los dispositivos, los usuarios

ANEXOS
DIVISIÓN DE CONTRATOS

- Reporte del top veinte (20) sitios web permitidos.
- Reporte del top veinte (20) categorías bloqueadas.
- Reporte del top veinte (20) categorías permitidas.
- Reporte del top veinte (20) de IP/Usuarios con mayor navegación a Internet.
- Reporte del top veinte (20) de IP/Usuarios con mayor consumo de ancho de banda.

4.4.2.3.7 Antispam

- Reporte de la disponibilidad de los activos de infraestructura (Antispam), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (Antispam), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (Antispam), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (Antispam), incluyendo tiempos de solución.
- Estadísticas de correos electrónicos bloqueados y recibidos.
- Reporte del top diez (10) de usuarios con mayor recepción de correo electrónico.
- Reporte del top diez (10) de usuarios con mayor envió de correo electrónico.
- Reporte del top diez (10) de dominios bloqueados (entrada/salida).
- Reporte del top diez (10) de dominios permitidos (entrada/salida).
- Reporte del top diez (10) de tamaño de información transferida por correo electrónico (entrada/salida).
- Reporte del top diez (10) de virus identificados.

4.4.2.3.8 Antimalware

- Reporte de la matriz de riesgos a partir de los hallazgos encontrados.
- Reporte de tabla de hallazgos clasificados por su riesgo donde se integren los hallazgos encontrados indicando el número de eventos asociados y el impacto que estos causan.
- Reporte del inventario de los sistemas operativos monitoreados.
- Reporte con el detalle técnico de cada incidente detectado, y que integre:
  - Fecha y hora del incidente.
  - Dirección IP de origen, destino, puerto de origen y destino.
  - Dispositivos asociados con el incidente.
  - Usuario de directorio activo presente durante el momento del incidente (si aplica).
  - Clasificación del incidente.
  - Origen del ataque y destino del atacante (en caso de aplicar).
  - Sistema operativo origen.

4.4.2.3.9 Firewall Especializado en Servicios Web (WAF)

- Reporte de la disponibilidad de los activos de infraestructura (WAF), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (WAF), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (WAF), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (WAF), incluyendo tiempos de solución.
- Reporte del top diez (10) de ataques bloqueados.
- Reporte del top diez (10) de portales con más ataques.
- Reporte de top diez (10) de consumo de ancho de banda.

4.4.2.4 Entregables bajo demanda

KIO NETWORKS generará bajo demanda los siguientes documentos y/o reportes, a solicitud del órgano de gobierno que señale el Instituto; y que incluyen de manera enunciativa más no limitativa los siguientes conceptos:

4.4.2.4.1 Servicios de Control de Calidad

4.4.2.4.1.1 Análisis de Vulnerabilidades

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados, así como el plan de mitigación propuesto.
- Archivos electrónicos (MS Excel) con la información fuente obtenida de las herramientas tecnológicas que se utilizaron para realizar los escaneos de vulnerabilidades.
- Reporte de los escaneos de vulnerabilidades realizados, indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja).

4.4.2.4.1.2 Pruebas de Penetración

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura verificados, así como el plan de mitigación propuesto.

- Reporte del top diez (10) de los protocolos permitidos.
- Reporte de reglas de control de acceso más utilizadas.
- Reporte del top diez (10) de direcciones IP Públicas/Privadas con más consumo de ancho de banda.

4.4.2.3.2 IPS

- Reporte de la disponibilidad de los activos de infraestructura (IPS), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (IPS), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (IPS), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (IPS), incluyendo tiempos de solución.
- Reporte de promedio de tráfico de entrada/salida.
- Reporte del top diez (10) de intentos ataques detectados y bloqueados (firmas).
- Reporte del top diez (10) de equipos que generar tráfico anómalo.
- Reporte del top diez (10) de usuarios que generan tráfico anómalo.

4.4.2.3.3 Anti-denegación de Servicios (DDoS)

- Reporte de la disponibilidad de los activos de infraestructura (AntiDDoS), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (AntiDDoS), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (AntiDDoS), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (AntiDDoS), incluyendo tiempos de solución.
- Reporte del top diez (10) de anomalías clasificadas por nivel de severidad.
- Reporte del top diez (10) de activos de infraestructura con mayor número de incidencias de tráfico anómalo (internos/externos).
- Reporte del top diez (10) de protocolos bloqueados.

4.4.2.3.4 Redes Privadas Virtuales – VPN (C2S – S2S)

- Reporte de la disponibilidad de los activos de infraestructura (Concentrador VPN), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (Concentrado VPN), incluyendo tiempo de atención.

- Reporte de incidentes atendidos en los activos de infraestructura (Concentrador VPN), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (Concentrador VPN), incluyendo tiempos de solución.
- Reporte del top diez (10) usuarios que se conectan a través de VPN C2S.
- Reporte del top diez (10) de servicios (direcciones IP destino) que se conectan a través de VPN C2S y S2S.
- Reporte del top diez (10) de ancho de banda consumido por VPN S2S.

4.4.2.3.5 Gestión Unificada de Amenazas (UTM)

- Reporte de la disponibilidad de los activos de infraestructura (UTM), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (UTM), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (UTM), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (UTM), incluyendo tiempos de solución.
- Reporte del top diez (10) de los protocolos bloqueados.
- Reporte del top diez (10) de los protocolos permitidos.
- Reporte del top diez (10) de intentos ataques detectados y bloqueados (firmas).
- Reporte del top diez (10) de equipos que generar tráfico anómalo.
- Reporte del top veinte (20) sitios web bloqueados.
- Reporte del top veinte (20) sitios web permitidos.
- Reporte del top veinte (20) de IP/Usuarios con mayor navegación a Internet.
- Reporte del top diez (10) de servicios (direcciones IP destino) que se conectan a través de VPN.

4.4.2.3.6 Filtrado de Contenido Web

- Reporte de la disponibilidad de los activos de infraestructura (Filtrado de Contenido Web), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (Filtrado de Contenido Web), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (Filtrado de Contenido Web), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (Filtrado de Contenido Web), incluyendo tiempos de solución.
- Reporte del top veinte (20) sitios web bloqueados.

ANEXOS

DIVISIÓN DE CONTRATOS

Llevar a cabo todas las tareas necesarias para la revisión de los equipos en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Revisar y validar en conjunto con el Instituto los requerimientos de protección, inspección de contenido http o https y seguridad de aplicativos web, tal y como sea solicitado.

Aprovisionar nuevos servicios aplicativos que requieran la protección a través del WAF, conforme el Instituto lo necesite, siempre y cuando las capacidades del equipo lo soporten, en cuyo caso el instituto solicitará una unidad de consumo adicional.

Integrar diseño, soporte de cambios y reingenierías en WAF.

Monitorear y optimizar el uso de los servicios de WAF.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Firewall Especializado en Servicios Web (WAF) relacionados para al menos:

- Cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución, configuradas para los servicios web públicos y/o privados.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, **KIO NETWORKS** realizará la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

4.4.2.2 Entregables de única ocasión

4.4.2.2.1 Centro de Operaciones de Seguridad (SOC)

- Diseño físico y lógico de alto nivel con la descripción detallada de la arquitectura propuesta para habilitar los servicios de la solución de seguridad.
- Copia de los siguientes procesos de seguridad que tiene implementados en el "SOC":
  - Proceso de Administración y Control de Cambios.
  - Proceso de Disponibilidad.
  - Proceso de Administración de Vulnerabilidades.
  - Proceso de Atención y Respuesta a Incidentes.
  - Proceso de Mejora Continua.
- La matriz de escalamiento del servicio tanto técnico como jerárquica.
- Procesos de la Mesa de Servicio, que se indican a continuación:
  - Administración de incidentes.
  - Administración de problemas.
  - Administración de cambios y configuraciones.
  - Administración de liberaciones.
- Metodología para el proceso de administración de vulnerabilidades.
- Procedimientos de seguridad aplicados en el "SOC" para:
  - Manejo de alarmas.
  - Atención y Respuesta a Incidentes de Seguridad

4.4.2.3 Entregables Periódicos

KIO NETWORKS generará de manera integrada un **Entregable Mensual del Servicio de Seguridad**, que incluya de manera enunciativa más no limitativa los siguientes conceptos:

- Servicios de Operación

4.4.2.3.1 Firewall

- Reporte de la disponibilidad de los activos de infraestructura (firewall), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (firewall), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (firewall), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (firewall), incluyendo tiempos de solución.
- Reporte de promedio de tráfico de entrada/salida por cada DMZ asignada.
- Reporte del top diez (10) de los protocolos bloqueados.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

Llevar a cabo todas las tareas necesarias para la revisión del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante. Siempre y cuando esté autorizado por el Instituto.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Conocer y entender las políticas actuales de seguridad del Instituto, particularmente aquellas relacionadas con el manejo de información.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Filtrado de Contenido de Correo relacionados con al menos:

- Cumplimiento de las políticas de reglas de acceso a la información.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución, configuradas para las cuentas de usuario.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución de Filtrado de Contenido de Correo, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, **KIO NETWORKS** realizará la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

4.4.2.1.8 Antimalware

Descripción del servicio:

El Instituto requiere de un servicio de detección y protección contra amenazas avanzadas en la red interna. La infraestructura propuesta será de última generación y dedicada exclusivamente para las necesidades del Instituto y cumplirá con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de mejora de los equipos de Antimalware en la arquitectura de seguridad y comunicaciones.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

Llevar a cabo todas las tareas necesarias para la revisión del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Antimalware relacionados para al menos:

- Cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución, configuradas para el tráfico externo y/o interno.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, **KIO NETWORKS** realizará la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

4.4.2.1.9 Firewall Especializado en Servicios Web (WAF)

Descripción del servicio:

KIO NETWORKS ofrecerá el servicio de protección, prevención y control de ataques para aplicativos web expuestos en Internet. La infraestructura propuesta será de última generación y dedicada exclusivamente para las necesidades del Instituto y cumplirá con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de mejora de los equipos de Firewall Especializado en Servicios Web (WAF) en la arquitectura de seguridad y comunicaciones.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

ANEXOS
DIVISIÓN DE CONTRATOS

KIO NETWORKS asegurará que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.

KIO NETWORKS prevendrá la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

KIO NETWORKS atenderá todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

KIO NETWORKS emitirá alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Gestión Unificada de Amenazas (UTM) relacionados para al menos:

- Cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, **KIO NETWORKS** realizará la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

4.4.2.1.6 Filtrado de Contenido Web

Descripción del servicio:

KIO NETWORKS ofrecerá el servicio de filtrado de contenido Web mediante políticas de acceso que permita controlar y filtrar la utilización del servicio de acceso a Internet, en función de roles y perfiles. La infraestructura propuesta será de última generación y dedicada exclusivamente para las necesidades del Instituto y cumplirá con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de mejora de los equipos de Filtrado de Contenido Web en la arquitectura de seguridad y comunicaciones.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

Llevar a cabo todas las tareas necesarias para la revisión de los equipos en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante. Siempre y cuando esté autorizado por el Instituto.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Filtrado de Contenido de Correo relacionados con al menos:

- Cumplir las políticas de reglas de acceso a la información.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución, configuradas para las cuentas de usuario.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución de Filtrado de Contenido Web, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

La solución ofertada incluye el licenciamiento necesario para soportar 120,000 usuarios de manera simultánea.

Acordar con el Instituto el tipo de implementación que se integrará para el uso de los servicios (modo implícito o explícito), y en su caso, podrá solicitar modificaciones al uso del mismo conforme las necesidades operativas así lo demanden.

4.4.2.1.7 Antispam

Descripción del servicio:

KIO NETWORKS ofrecerá el servicio de analizar correos electrónicos de entrada y salida con el objetivo de bloquear amenazas de spam, malware, phishing, amenaza persistente avanzada (Advanced Persistent Threat APT's), reputación de URLs embebidas en los correos. La infraestructura propuesta será de última generación y dedicada exclusivamente para las necesidades del Instituto y cumplirá con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de mejora de los equipos de Filtrado de Contenido de Correo Electrónico (Antispam) en la arquitectura de seguridad y comunicaciones.

KIO NETWORKS atenderá todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

KIO NETWORKS emitirá alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Anti-denegación de Servicios (DDoS) relacionados para al menos:

- Cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, **KIO NETWORKS** realizará la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

4.4.2.1.4 Redes Privadas Virtuales – VPN (C2S – S2S)

Descripción del servicio:

El Instituto requiere del Servicio de interconexión a través de Internet que permitan establecer comunicación desde localidades remotas para la transferencia de información a través de un canal cifrado.

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de mejora de los equipos para Redes privadas Virtuales – VPN en la arquitectura de seguridad y comunicaciones.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

Llevar a cabo todas las tareas necesarias para la revisión de los equipos en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Gestionar el alta de accesos remotos debida y previamente autorizados por el Instituto a través de los mecanismos y personal que para ello designe este último.

Solicitar de manera mensual la lista de usuarios dados de baja de la organización y proceder a la deshabilitación de sus accesos remotos de manera inmediata.

Reportar bajo demanda la lista de usuarios y entidades (terceros) que cuentan con acceso remoto VPN C2S – S2S.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Redes privadas Virtuales – VPN relacionados para al menos:

- Cumplir las políticas de reglas de acceso a la información.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución, configuradas para las cuentas de usuario o servicios con terceros.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, **KIO NETWORKS** realizará la sustitución de componentes tecnológicos por otros de igual o mejores características/funcionalidades.

4.4.2.1.5 Gestión Unificada de Amenazas (UTM)

Descripción del servicio:

KIO NETWORKS ofrecerá un servicio de protección perimetral especializada en control de acceso, prevención de intrusos, Filtrado de Contenido Web y VPN, para control de tráfico y detección de actividad anómala. La infraestructura propuesta será de última generación y dedicada exclusivamente para las necesidades del Instituto y cumplirá con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

KIO NETWORKS definirá en conjunto con el Instituto la estrategia de mejora de los equipos de Gestión Unificada de Amenazas (UTM) en la arquitectura de seguridad y comunicaciones.

KIO NETWORKS llevará a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

KIO NETWORKS acordará con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

KIO NETWORKS integrará cada dispositivo hacia su respectiva consola de administración.

ANEXOS

DIVISIÓN DE CONTRATOS

- Notificar sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución.
- Notificar aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, **KIO NETWORKS** realizará la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades.

4.4.2.1.2 IPS

Descripción del servicio:

KIO NETWORKS ofrecerá el servicio de protección perimetral basado en firmas y que identifiquen vulnerabilidades, para contener los intentos de obtener acceso a los recursos o servicios publicados en Internet o Intranet que pudieran afectar la operación de la organización, detectar accesos no autorizados y prevenir fugas de información. La infraestructura propuesta será nueva, de última generación y dedicada exclusivamente para las necesidades del Instituto y cumplirá con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de mejora en los Equipos ya existentes de Sistema de Prevención de Intrusos (IPS por sus siglas en inglés) en la arquitectura de seguridad y comunicaciones.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

Llevar a cabo todas las tareas necesarias para la revisión de los equipos en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante. Siempre y cuando esté autorizado por el Instituto.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Prevención de Intrusos relacionados para al menos:

- Cumplir las políticas de reglas de acceso a la información.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, **KIO NETWORKS** realizará la sustitución de componentes tecnológicos por otros de igual o mejores características/funcionalidades.

4.4.2.1.3 Anti-denegación de Servicios (DDoS)

Descripción del servicio:

El Instituto requiere de un servicio de protección contra ataques de Denegación de Servicio Distribuido que se encuentren basados en firmas y volúmenes de conexión altos. La infraestructura propuesta será de última generación y dedicada exclusivamente para las necesidades del Instituto y cumplirá con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

KIO NETWORKS definirá en conjunto con el Instituto la estrategia de mejora de los equipos de Anti-denegación de Servicios (DDoS) en la arquitectura de seguridad y comunicaciones.

KIO NETWORKS habilitará esquema de Alta Disponibilidad (HA por sus siglas en inglés).

KIO NETWORKS llevará a cabo todas las tareas necesarias para la revisión del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

KIO NETWORKS acordará con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

KIO NETWORKS integrará cada dispositivo hacia su respectiva consola de administración.

KIO NETWORKS asegurará que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.

KIO NETWORKS prevendrá la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

- Número directo de las instalaciones del SOC.
- Correo Electrónico

El personal que KIO Networks integre y que se relaciona en puntos anteriores, contará con experiencia probada en las áreas de tecnología y de seguridad de la información que se indica:

- Curriculum vitae de todo el personal deberá indicar al menos:
- Experiencia profesional: bajo este rubro, se considerarán todos los cargos que cada integrante haya desempeñado, con fecha, nombre de los empleadores, nombre de los cargos que ha ejercido y el tipo de funciones bajo su responsabilidad.
- Experiencia en proyectos de su especialidad en Seguridad de la Información: bajo este rubro se citarán y describirán todos los proyectos que el integrante ha participado, y contará con experiencia comprobable de cuando menos 2 años.
- Estudios: bajo este rubro se anotarán todos los estudios en materia de seguridad de la información, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica. Las certificaciones son de tecnología y/o de seguridad de tipo "vendor-neutral".
- Incluir la estructura del grupo de trabajo, indicando por cada perfil las responsabilidades y competencias.
- El Instituto podrá solicitar la revisión de la infraestructura de seguridad por un tercero en cualquier momento, durante la vigencia del contrato, a fin de dar certeza de la entrega del servicio.
  - Generación de reportes derivados de la falla en algún componente de la infraestructura de seguridad, la cual deberá contener por lo menos:
  - Infraestructura afectada y servicios asociados
  - Causa raíz
  - Remediación o medidas compensatorias propuestas en tanto se identifica la causa raíz
  - Impacto e indisponibilidad del servicio afectado

Las credenciales y capacidades que deberán cubrir los recursos asignados al proyecto se indican en el apéndice correspondiente.

Consideraciones generales para los servicios de soporte del SSNI

4.4.2.1 Administración y soporte de componentes de seguridad

Como referencia de los servicios que son proporcionados actualmente, se puede consultar las especificaciones técnicas en el apéndice correspondiente.

4.4.2.1.1 Firewall

Descripción del servicio:

El Instituto requiere de la seguridad y protección de control de acceso, bloqueo contra ataques dirigidos a las aplicaciones e inspección sobre los paquetes a nivel de aplicación para identificar patrones de tráfico anómalo. La infraestructura propuesta será de última generación y dedicada exclusivamente para las necesidades del Instituto y cumplirá **KIO NETWORKS** con las siguientes especificaciones técnicas mínimas:

Detalles del Servicio:

Definir en conjunto con el Instituto la estrategia de habilitación de los Firewalls en la arquitectura de seguridad y comunicaciones.

Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).

Llevar a cabo todas las tareas necesarias para la revisión de los equipos en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el Instituto.

Acordar con el personal del Instituto todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.

Integrar cada dispositivo hacia su respectiva consola de administración.

Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante. Siempre y cuando esté autorizado por el Instituto.

Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes o nubes.

Proporcionar el acceso a servicios ubicados en la capa de servidores del centro de datos (DMZs), realizando la gestión de acuerdo al esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

Realizar traducciones de direcciones IP homologadas para garantizar la seguridad de servidores.

Gestionar las reglas y objetos requeridos para la protección de los flujos del Instituto.

Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Firewalls relacionados para al menos:

- Cumplir las políticas de reglas de acceso a la información.

ANEXOS

DIVISIÓN DE CONTRATOS

- Contará con la capacidad de manejo de al menos 512 Vlans.
- Deberá poder operar de manera transparente como un dispositivo Capa 2 y como un dispositivo de ruteo en Capa 3.
- Deberá operar en alta disponibilidad tomando en cuenta los siguientes esquemas.
  - Modo ruteo en capa 3 Activo-Activo
  - Modo ruteo en capa 3 Activo-Pasivo
  - Modo balanceo de carga y conmutación por error.
  - Modo VRRP
- Incluirá la capacidad de generar al menos 10,000 túneles VPN a través del protocolo IPSec.
- Deberá poder aplicar QoS (Quality of Service) para priorizar tráfico de Datos, Voz y Video
- Deberá poder crear políticas granulares, es decir:
  - Para usuarios
  - Para grupos

Además, identificará, permitirá, bloqueará o limitará el uso de aplicaciones independientemente del puerto, protocolo o técnica evasiva.

- Permitirá el escaneo de aplicaciones tales como mensajería instantánea, redes sociales, streaming de video, Voz sobre IP, juegos entre otras.
- Deberá poder realizar autenticación de usuarios a través de Directorio Activo (LDAP), Portal Cautivo, Kerberos, Radius, Tacacs.
- Contará con la administración centralizada de acceso a usuarios, a los recursos del Instituto y aplicaciones en Internet
- Permitirá la conexión a las aplicaciones del Instituto a través de dispositivos móviles (Tablet's, SmartPhone's)

4.4.2 Soporte para la Operación de la Seguridad de la Nube IMSS

Descripción del Servicio:

El Instituto requiere que **KIO NETWORKS** cuente con un Centro de Operaciones de la Seguridad (SOC) totalmente funcional en la actualidad, que se encuentre físicamente en las instalaciones de **KIO NETWORKS**. El objetivo de este centro será la gestión de la seguridad y responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad, que ejecute actividades de revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, análisis forense, notificación de alertas y vulnerabilidades, así como el establecimiento de acciones de mejora sustentable.

Detalles del Servicio:

Ubicarse dentro de territorio mexicano (a fin de que se encuentre dentro de jurisdicción de las leyes mexicanas)

Contar con un mecanismo que garantice la continuidad de la operación frente a contingencias

INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

Operación 7x24x365 días durante la vigencia del contrato.

Personal en sitio y remoto altamente calificado con las credenciales requeridas para la administración y monitoreo de los componentes que integran la solución.

Mantenimiento de las suscripciones a sitios y listas de correos de internet que alertan de nuevas vulnerabilidades.

Infraestructura dedicada para la administración, operación y monitoreo de los componentes hardware y software.

Revisión continúa a la configuración implementada en los dispositivos de seguridad. La finalidad es identificar errores, depurar reglas, optimizar el desempeño de los componentes hardware y software, así como mantener las configuraciones en cumplimiento con los requisitos de seguridad que establece la normatividad y estándares aplicables.

Acciones correctivas y preventivas para asegurar la confidencialidad, integridad y disponibilidad de la información.

Notificaciones y alertas personalizadas, en caso de desviaciones, anormalidades o brechas de seguridad.

Personal especializado en revisiones de seguridad en infraestructura y aplicaciones.

Revisiones continuas a la operación del SOC, que permitan establecer mejora en los procesos, procedimientos y controles de seguridad.

Atención y Respuesta a Incidentes de Seguridad.

Soporte y Atención a fallas a los componentes hardware y software que integran la solución.

Monitorear la disponibilidad de los componentes hardware y software que integran la solución ofertada. La solución de monitoreo debe tener la capacidad de generar alertas y notificaciones en caso de fallas, degradación de los signos vitales, intermitencia y/o pérdida de disponibilidad.

Mantenimiento preventivo y correctivo a la solución instalada.

Administración de Dispositivos.

Administración de Requerimientos.

Administración de Cambios.

Administración de Configuraciones.

Administración de Vulnerabilidades.

Administración de Incidentes.

Administración de Problemas.

Investigación de Incidentes.

Mesa de servicio apegada a ITIL v3.

El servicio de soporte a fallas permitirá el levantamiento de tickets a través de los siguientes medios:

INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

4.4.1.9 Servicio de Seguridad Perimetral para Enlaces de Banda Ancha

El Instituto requiere un servicio que permita proporcionar la infraestructura que brinde seguridad perimetral para enlaces de banda ancha, a través de los cuales se establece la transferencia de información entre diferentes unidades médicas y administrativas del IMSS.

El servicio de seguridad perimetral para enlaces de banda ancha se requiere en dos modalidades:

- Sitios con un ancho de banda mayor a 100 Mbps y hasta 1 Gbps
- Sitios con un ancho de banda de hasta 100 Mbps.

Las características principales que debe reunir el servicio para Sitios con un ancho de banda mayor a 100 Mbps y hasta 1 Gbps:

- Contará al menos con un rendimiento de 8 Gbps, en su funcionalidad de firewall.
- Tendrá al menos un rendimiento 1.2 Gbps en su funcionalidad de IPS
- Mínimo contará con 12 puertos 100/1000 de cobre RJ45
- Mínimo contará con 4 puertos de 1 Gbps de fibra
- Mínimo contará con 2 puertos de 10 Gbps de fibra
- Será un dispositivo de nivel empresarial
- Será un dispositivo multifuncional, es decir integrar las funcionalidades descritas a continuación, en un solo dispositivo dedicado:
  - Firewall
  - Detección y prevención de intrusos (IPS)
  - Filtrado de contenido de la WEB
  - Detección y control de virus
  - Detección y control de amenazas y programas maliciosos
  - Protección para correo electrónico
  - Detección y control de correo no deseado
- Contará con una consola de administración integrada accesible vía remota y a través de interfaz RJ45
- Contará con doble fuente de poder que pueda ser sustituida en caliente sin afectar al dispositivo y al servicio que presta
- Garantizará técnicamente la seguridad de datos, en situaciones como accesos remotos y comunicaciones de sitio a sitio
- Será compatible con direccionamiento IPv4 e IPv6
- Contará con la capacidad de manejo de al menos 1024 vLANs.
- Deberá poder operar de manera transparente como un dispositivo Capa 2 y como un dispositivo de ruteo en Capa 3.
- Deberá operar en alta disponibilidad tomando en cuenta los siguientes esquemas

  - Modo ruteo en capa 3 Activo-Activo
  - Modo ruteo en capa 3 Activo-Pasivo
  - Modo balanceo de carga y conmutación por error.
  - Modo VRRP
- Incluirá la capacidad de generar al menos 15,000 túneles VPN a través del protocolo IPSec.
- Deberá poder aplicar QoS (Quality of Service) para priorizar tráfico de Datos, Voz y Video
- Deberá poder crear políticas granulares, es decir:
  - Para usuarios
  - Para grupos

Además, identificará, permitirá, bloqueará o limitará el uso de aplicaciones independientemente del puerto, protocolo o técnica evasiva.

- Permitirá el escaneo de aplicaciones tales como mensajería instantánea, redes sociales, streaming de video, Voz sobre IP, juegos entre otras.
- Deberá poder realizar autenticación de usuarios a través de Directorio Activo (LDAP), Portal Cautivo, Kerberos, Radius, Tacacs.
- Contará con la administración centralizada de acceso a usuarios, a los recursos del Instituto y aplicaciones en Internet
- Permitirá la conexión a las aplicaciones del Instituto a través de dispositivos móviles (Tablet's, SmartPhone's)

Las características principales que debe reunir el servicio para Sitios con un ancho de banda de hasta 100 Mbps:

- Contará al menos con un rendimiento de 3 Gbps, en su funcionalidad de firewall.
- Tendrá al menos un rendimiento 600 Mbps en su funcionalidad de IPS
- Mínimo contará con 8 puertos 100/1000 de cobre RJ45
- Mínimo contará con 4 puertos de 1 Gbps de fibra
- Será un dispositivo de nivel empresarial
- Será un dispositivo multifuncional, es decir integrar las funcionalidades descritas a continuación, en un solo dispositivo dedicado:
  - Firewall
  - Detección y prevención de intrusos (IPS)
  - Filtrado de contenido de la WEB
  - Detección y control de virus
  - Detección y control de amenazas y programas maliciosos
  - Protección para correo electrónico
  - Detección y control de correo no deseado
- Contará con una consola de administración integrada accesible vía remota y a través de interfaz RJ45
- Garantizará técnicamente la seguridad de datos, en situaciones como accesos remotos y comunicaciones de sitio a sitio
- Será compatible con direccionamiento IPv4 e IPv6

ANEXOS

DIVISIÓN DE CONTRATOS

- Verificación de requerimientos contractuales y legales
- Identificación de los requerimientos internos y externos
- Validación de aplicabilidad de los requerimientos
- Formato para la Autorización para implantar y operar el Sistema de Gestión de Seguridad de la Información
- Preparación de la Declaración de Aplicabilidad
- Documentar los objetivos de control y los controles elegidos y la justificación de su elección
- Documentar los controles actualmente implementados
- Documentar la exclusión de controles y la justificación de su exclusión
- Implementar y Operar el Sistema de Gestión de Seguridad de la Información

Análisis de Riesgos de Seguridad de la Información

- Realización del análisis de riesgo con base en lo definido en el servicio de gestión de riesgos de seguridad.
  - Generación del plan de tratamiento de riesgos. La metodología contempla los siguientes puntos:
- Identificación de las acciones a realizar por parte de la organización y su administración
- Identificación de los recursos necesarios y prioridades
- Identificación de las responsabilidades para administrar los riesgos de seguridad de la información
- Aplicación del plan de tratamiento de riesgos. La metodología contempla los siguientes puntos:

Asignación de los roles y responsabilidades en la implantación de los controles relativos a personas, procesos y tecnología involucrados en la mitigación de los riesgos.

  - Actualización de documentación. Alineada a los requisitos establecidos en el proceso ASI y OPEC de MAAGTIC SI.
- Afinación de políticas y procedimientos de seguridad existentes
- Definición del proceso de reporte y atención de incidentes de seguridad (ERISC)
  - Propuestas de implementación de los controles seleccionados: La metodología contempla los siguientes puntos:
    - Control de accesos
    - Monitoreo de cuentas
    - Definición del proceso de Continuidad del negocio
- Implantación de los Roles y responsabilidades definidas para el Sistema de Gestión de Seguridad de la Información
- Controles de seguridad en la infraestructura tecnológica de acuerdo a lo definido en el alcance.
  - Administración del cambio cultural. La metodología contempla los siguientes puntos:
- Desarrollo de un Programa de concientización con usuarios y operadores del Sistema de Gestión de Seguridad de la Información
- Determinación de las necesidades de capacitación para el personal que administra el Sistema de Gestión de Seguridad de la Información
- Apoyo en la capacitación relativa a temas de seguridad de la información.

  - Manual de Gestión de Seguridad de la Información. Se documentará un manual que contiene las referencias de la documentación generada en esta fase para dar trazabilidad al de las cláusulas de la norma
- Monitorear y Revisar el Sistema de Gestión de Seguridad de la Información
  - Revisiones gerenciales. La metodología contempla los siguientes puntos:
- Los dueños del proceso deberán hacer una revisión al Sistema de Gestión de Seguridad de la Información a fin de verificar que los objetivos del Sistema de Gestión de Seguridad de la Información están alineados a los objetivos de negocio en materia de seguridad de la información y que garantizan el adecuado manejo de los riesgos existentes.
- **KIO NETWORKS** generará el procedimiento de revisiones gerenciales.
- **KIO NETWORKS** propondrá los formatos requeridos para llevar a cabo las revisiones
  - Auditorías internas. La metodología contempla lo siguiente:
- Apoyo en la generación del plan de auditorías internas a las áreas de TI y a los terceros que proveen servicios de TI al Instituto.
- Definición de los formatos requeridos para llevar a cabo las auditorías
- Aplicación de una auditoría interna al Sistema de Gestión de Seguridad de la Información para verificar el cumplimiento con el estándar ISO/IEC 27001:2013 y a los procesos de seguridad ASI y OPEC del MAAGTICSI
  - Mantener y Mejorar el Sistema de Gestión de Seguridad de la Información
- Implementación de mejoras. Contempla los siguientes puntos:
  - Priorización de las acciones correctivas y no conformidades identificadas en las revisiones gerenciales, revisiones independientes, auditorías internas y revisiones técnicas
  - Identificación de los responsables de llevar a cabo las mejoras por parte de la organización.
  - El Instituto definirá las fechas compromiso para la terminación de las mejoras, únicamente para seguimiento interno.
- Tomar acciones correctivas y en las no conformidades. Contempla los siguientes puntos:
- Apoyo en la definición del procedimiento para realizar acciones correctivas y no conformidades derivadas de las auditorías.
- Definición del formato para llenado de acciones correctivas y no conformidades.
- Coordinación de la ejecución de las acciones correctivas ya definidas y en su caso las no conformidades que se identifiquen.
- Comunicar los resultados de las acciones tomadas. Contempla el siguiente punto:
  - Apoyo en la programación de reuniones de seguimiento al Sistema de Gestión de Seguridad de la Información para dar a conocer el alcance de las acciones correctivas y no conformidades realizadas y verificar su apego a los requerimientos de los dueños de la información y a los involucrados en los procesos del Instituto.

4.4.1.7 Análisis de Riesgos de Seguridad de la Información

Descripción del servicio:

Identificar, evaluar y manejar los riesgos de la seguridad de la información, utilizando técnicas estadísticas, información histórica, fuentes de información especializada y otras que permitan, determinar la exposición a diferentes escenarios de riesgo, probabilidad e impacto, así como las recomendaciones y líneas de acción, que permitan alcanzar un nivel de seguridad aceptable a un costo razonable enfocado al catálogo de infraestructuras críticas del Instituto.

Detalles del Servicio:

KIO NETWORKS cumplirá con al menos las siguientes funcionalidades operativas:

- Contexto
  - Recopilar información sobre las operaciones del Instituto, las relaciones entre los procesos de negocio, procesos y recursos de tecnología, las dependencias entre estos, tomando en cuenta:
    - Consideraciones generales del Instituto
    - Definición de criterios básicos para la ejecución del análisis
    - Definición del alcance del análisis
    - Definición del equipo de trabajo de **KIO NETWORKS** y del Instituto que participará en la ejecución del análisis.
- Valoración de riesgos
  - Utilizar la metodología basada en el proceso ASI del MAAGTICSI para la gestión de riesgos de seguridad. La metodología contendrá:
    - Identificación activos, considerando como activos a los procesos, actividades, información, infraestructura, y gente.
    - Identificación de vulnerabilidades.
    - Identificación de amenazas.
    - Escenarios de riesgo.
    - Priorización del riesgo.
- Tratamiento de los riesgos
  - Criterios para la atención del riesgo identificando y analizando varias opciones de tratamiento de las cuales se elegirá la que mejor balance costo-beneficio genere, considerando el resultado obtenido:
    - Evitar.
    - Mitigar.
    - Transferir.
    - Aceptar.
- Seguimiento y Mitigación de riesgos
  - Deberá dar seguimiento a los planes de tratamiento de riesgos conforme lo siguiente:

- La generación de los planes de mitigación de riesgos
- Identificación de los responsables de cada plan.
- Acompañamiento en la implementación de controles normativos.

4.4.1.8 Sistema de Gestión de Seguridad de la Información (SGSI)

Descripción del servicio:

Apoyar al Instituto en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado al MAAGTICSI y basado en el estándar ISO 27001, que permita emitir directivas en materia de seguridad de la información a las áreas de TI y a los terceros que soportan la operación de TI.

Detalles del Servicio:

KIO NETWORKS cumplirá con al menos las siguientes funcionalidades operativas:

- Planear
  - Capacitación inicial – Curso "Inducción a la norma 27001:2013. Curso introductorio que permite al participante:

Conocer la estructura de la norma ISO/IEC 27001:2013

Interpretar los requisitos solicitados para el cumplimiento de la norma

Conocer las etapas para la implementación de un SGSI

Generación de directivas de seguridad. Manual de políticas de seguridad de la información:

- Basadas en los dominios que establece la norma ISO 27001.
- Alineadas a los procesos de seguridad ASI y OPEC del MAAGTIC SI.
- Enfocadas a las áreas de TI y a los terceros que proveen servicios de TI al Instituto, considerando como alcance el catálogo de infraestructuras críticas del Instituto.

Identificación y valuación de activos (relacionado al catálogo de infraestructuras críticas) del proceso involucrado en el Sistema de Gestión de Seguridad de la Información. La metodología contempla los siguientes puntos:

- Identificación de los activos del proceso.
- Valoración de los activos del proceso.
- Identificación de requerimientos de seguridad.
- Identificación de los controles de seguridad existentes.

Generación de la Declaración de Aplicabilidad. (SoA: Statement of Applicability). La metodología contempla los siguientes puntos:

- Identificación y aplicabilidad de los requerimientos internos y externos.
- Selección de los objetivos de control y controles para el tratamiento de los riesgos

ANEXOS

DIVISIÓN DE CONTRATOS

- Parameters Tampering
- Cookie Poisoning
- Hidden Field Manipulation

- Criptografía
  - Fortaleza del algoritmo
  - Gestión de llaves
- Ataques Lógicos
  - Abuso de funcionalidades
  - Input Field Validation Checking
- Protección de Datos
  - Transporte
  - Almacenamiento
- Divulgación de Información
  - Indexado de directorio
  - Path Traversal
  - Manejo inseguro de errores
  - Comentarios HTML

4.4.1.5 Análisis Forenses

Descripción del servicio:

El Instituto requiere de un servicio de análisis de incidentes de seguridad para determinar y documentar en qué consistió a través de la integración de registros o bitácoras que permitan obtener indicios de eventos y su relación en el tiempo y que permitan identificar cuándo ocurrió, qué infraestructura, servicios tecnológicos o sistema de información fueron comprometidos, como fue realizado y quien estuvo relacionado con el incidente y el impacto del evento.

Detalles del Servicio:

KIO NETWORKS cumplirá con al menos las siguientes funcionalidades operativas:

- Apoyar en la definición del objetivo parámetros y cuestionario que resulten de interés para la investigación solicitada.
- Dar continuidad y seguimiento a los casos solicitados en un tablero de control, así como, el registro de los indicadores correspondientes.
- Preservar la integridad de la información recibida durante la ejecución del proceso de análisis forense.
- Participar en entrevistas y con los principales involucrados con la finalidad de obtener el contexto necesario en las investigaciones digitales realizadas.
- Obtener información de fuentes públicas en la red en caso de que estas pudieran llegar a ser relevantes para la investigación realizada.
- Realizar la evaluación de información en los puestos de servicio para la identificación de malware.
- Realizar un proceso de recuperación de información que haya sido borrada previamente.

- Proporcionar una herramienta colaborativa que facilite la visualización de hallazgos a los usuarios finales, así como generar reporte de hallazgos en caso de ser requerido

4.4.1.6 Borrado Seguro de Datos

Descripción del servicio:

Realizar el borrado seguro de información en servidores, equipos de centros de datos, discos duros externos y otras unidades de almacenamiento, que el Instituto solicite mediante una solución de borrado seguro que imposibilite, ante cualquier intento o medio, la recuperación de la información borrada, que permita la generación de un certificado que respalde la ejecución de borrado y que sea totalmente automatizada y gestionada centralmente.

Detalles del Servicio:

KIO NETWORKS cumplirá con al menos las siguientes funcionalidades operativas:

- Debe permitir realizar borrados completos en servidores derivados de sustitución de equipos, migraciones tecnológicas o retiro por finalización del contrato.
- Asegurará que los datos no puedan ser recuperados, basándose en al menos los siguientes estándares internacionales
  - HMG Infosec Standard 5 (baseline and enhanced),
  - opnavinst 5239.1ª
  - Extended NIST 800-88
  - DoD 5220.22-M
- Borrado de Discos duros IDE/ATA, SCSI, SAS, USB, SATA, Fiber Channel y FireWire de cualquier tamaño.
- Debe brindar la destrucción local y/o remota en múltiples dispositivos de almacenamiento
- Debe posibilitar el desmontaje RAID (SCSI)
- Debe permitir el borrado y detección de zonas bloqueadas / ocultas (DCO, HPA)
- Generará certificados de borrado infalsificables que ofrezcan protección ante cualquier instancia legal, en donde se incluya el resultado del proceso de borrado, fecha, hora, los datos del equipo, el detalle del HD borrado.
- Deberá emitir una firma electrónica para la autenticación de la integridad del reporte de Sanitización emitido por el software de borrado.
- La solución debe poder ejecutarse sin importar de qué sistema operativo se trate.
- El reporte que generé la solución deberá poder ser exportado a un medio de almacenamiento como USB o disco duro.

4.4.1.2 Pruebas y Validación

KIO NETWORKS integrará un área independiente a la que instala y opera los servicios de seguridad, cuya función será la de ser un punto de control de calidad de los servicios cuyo objetivo será validar que los mismos que vayan a entregar o ser entregados cumplan con los requerimientos y niveles de servicio solicitados por el Instituto.

El Instituto a través del área independiente del punto de control, solicitará la realización de pruebas a las diferentes arquitecturas del servicio de seguridad; lo anterior a fin de revisar que las diferentes arquitecturas tecnológicas de los servicios de seguridad operen con los niveles de disponibilidad y eficiencia, bajo las mejores prácticas de gestión para las Tecnologías de la Información y Comunicaciones.

KIO NETWORKS independiente del punto de control, podrá llevar a cabo verificaciones presenciales o remotas de los servicios ofrecidos a fin de dar certeza de que estos mismos se encuentran establecidos bajo las condiciones del presente contrato.

4.4.1.3 Análisis de Vulnerabilidades

Descripción del servicio:

El Instituto requiere de un servicio que permite ejecutar análisis técnicos especializados sobre los activos de infraestructura de procesamiento y redes que permitan identificar vulnerabilidades nuevas o conocidas.

Detalles del Servicio:

KIO NETWORKS cumplirá con al menos las siguientes funcionalidades operativas:

- Capacidad para integrarse al menos dos herramientas que permitan complementar los análisis de vulnerabilidad ejecutados.
- Capacidad para identificar los servicios a analizar, incluyendo el número de equipos involucrados y la versión de las plataformas de los sistemas.
- Identificación de vulnerabilidades documentadas en organismos internacionales como el CVE (Common Vulnerability Exposures).
- Identificación de configuraciones por omisión.
- Capacidad para determinar el grado de vulnerabilidad ante técnicas de ataque como:
  - SQL injection
  - Cross Site Scripting
  - Cross Site Request Forgery
  - Sensitive Data Exposure
  - Security Misconfiguration

  - Broken Authentication and Session Management
- Capacidad para elaborar un reporte técnico y/o ejecutivo donde se describa un riesgo asociado a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP llamada "OWASP risk rating Methodology", detallando recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.
- Capacidad para integrar un proceso/procedimiento de implementación de las medidas de remediación y recomendaciones realizadas, así como el integrar soporte técnico en la solución de los problemas presentados.
- Se dispondrá de un número ilimitado de eventos para realizar procesos de análisis de vulnerabilidades bajo demanda y conforme las necesidades operativas.

4.4.1.4 Pruebas de Penetración

Descripción del servicio:

El Instituto requiere de un servicio que permita realizar una serie de pruebas de penetración sobre la infraestructura del Instituto con el fin de buscar huecos o fallas en la seguridad establecida. Todas las pruebas serán realizadas con herramientas e ingenieros especializados.

Detalles del Servicio:

KIO NETWORKS cumplirá con al menos las siguientes funcionalidades operativas:

- Identificación los servicios o activos de información que sea analizarán, incluyendo el número de equipos involucrados, y la versión de las plataformas de los sistemas analizados.
- Identificación de vulnerabilidades y malas configuraciones.
- Explotación de acceso a los sistemas mediante el aprovechamiento de los huecos de seguridad detectados y/o vulnerabilidades detectadas.
- Evaluación de vulnerabilidades de al menos los siguientes rubros:
  - Autenticación y Autorización
    - Intentos ilimitados de inicio de sesión
    - Insuficiente autenticación
    - Insuficiente autorización
  - Gestión de sesión
    - Predicción de sesión
    - Secuestro de sesión
    - Reproducir sesión
    - Expiración de sesión insuficiente
  - Inyección de código
    - Inyección comando de SO
    - Inyección SQL
    - Cross-site Scripting
    - Inyección LDAP
    - Inyección HTML

ANEXOS
DIVISIÓN DE CONTRATOS

4.3.3.2.7 Gestión y control de la plataforma

KIO NETWORKS proporcionará un portal web seguro unificado para los productos y servicios que se solicitan dentro del servicio de publicación y contenido. Se cuentan con las siguientes herramientas, reportes, alertas, consola de administración y transferencia de conocimientos:

- El instituto proporciona los controles de accesos necesarios a la plataforma.
- Se proporciona al Instituto la visibilidad y el control de la infraestructura y los servicios propuestos en el presente Anexo técnico, como el estado de funcionamiento en todo momento e históricos diario, semanal, mensual; se logran ver los reportes hasta 3 meses atrás a la fecha de consulta.
- Se proporcionan alertas que informan directamente al Instituto cuando los umbrales definidos se han rebasado, lo que indica que el rendimiento y la experiencia del usuario se han degradado.
- Se provee monitoreo en tiempo real y con las capacidades de generar reportes históricos que ayudan en la evaluación y el mantenimiento de la eficacia de los portales y con su rendimiento, así como con el análisis de los patrones del tráfico de entrega tanto del lado de la infraestructura del Instituto como de la red o plataforma propuesta.
- Proveerá de una vista unificada de la solución incluyendo los tiempos promedio de respuesta y disponibilidad por locación, análisis de error con la capacidad de profundizar por cada página, por objetos en cada página, por códigos de respuesta http, tamaño y suma por cada ítem, dirección de IP del visitante.

4.3.4 Servicios eventuales

A lo largo del **Servicio de Integralidad y Telecomunicaciones**, se señalan una serie de servicios que pueden ser consumidos de manera eventual. Dichos servicios serán cotizados de manera individual según se señala en la sección Catálogo de Servicios.

4.3.5 Servicios extendidos

Conforme a lo señalado en la sección **Elementos Comunes de los Servicios**, los servicios extendidos se derivan del **Servicio de Integralidad y Telecomunicaciones**, del Punto Neutro de la Nube Hibrida y del Nodo de Extensión de Nube Privada en Modalidad Grande.

4.4 Servicio de Operación y Calidad de la Seguridad Informática Perimetral

4.4.1 Soporte para la Calidad de la Seguridad de la Nube IMSS

4.4.1.1 Diseño de Arquitectura de seguridad

Con la finalidad de obtener los mejores servicios de seguridad de la información, el área independiente de punto de control de calidad deberá valorar y en caso necesario actualizar el diseño de la arquitectura del servicio de seguridad, considerando los elementos necesarios para proporcionar la confidencialidad, integridad y disponibilidad de los activos de tecnologías de información y comunicaciones del Instituto.

Esta estrategia permitirá consolidar la integración de servicios, funciones, sistemas e infraestructura tecnológica en busca de mayor eficiencia, productividad y economías de escala.

En lo referente a la administración y control de la seguridad informática, se requiere el diseño de una arquitectura tecnológica integral que tenga por objetivo proveer servicios informáticos e infraestructura tecnológica que operen con altos niveles de disponibilidad y eficiencia, bajo las mejores prácticas de gestión para las Tecnologías de la Información y Comunicaciones.

Esta arquitectura tecnológica integral se conforma por 8 arquitecturas específicas y un centro de operación de la seguridad, que estructuran y dan orden a los diferentes elementos tecnológicos de forma congruente y consistente, para que "el Instituto" obtenga el mayor beneficio en términos de seguridad de la información en el uso de la tecnología.

Estas arquitecturas específicas son:

- Arquitectura de Firewall
- IPS
- DDoS
- Redes Privadas Virtuales
- UTM's
- Filtrado de contenido web
- Antispam
- Antimalware
- Web Access Firewall
- Centro de Operación de la Seguridad

Lo anterior permitirá contar con aplicaciones y sistemas de información segura por diseño y construcción, protegidos y monitoreados en producción. Identificando oportunamente el manejo de las vulnerabilidades, riesgos y amenazas en la infraestructura tecnológica y sus servicios. Proporcionando la administración y soporte con personal informático calificado con sólidos conocimientos y habilidades en el manejo de seguridad de la información.

- Control de acceso. Funcionalidad para controlar las identidades, proveer autenticación, autorización, y proveer un marco de trabajo para autenticación.
- Correlación de eventos y sistemas de seguridad. Funcionalidad que detecta e integra todos los eventos de autenticaciones, errores, eventos de seguridad, etc. Habilita auditoría de dichos eventos, así como la correlación y remediación de ataques informáticos a nivel del nodo de ENP.
- Gestión de equipo de cómputo. Funcionalidad de gestión de equipo de cómputo ya sea de escritorios virtuales, "zero clients" o equipos de escritorio. Este servicio facilitará la configuración, soporte técnico, gestión de seguridad e inventario de hardware y software; todo esto con el fin de tener mejor control sobre todos los activos que son parte del nodo NEP. Cada usuario podrá tener asignada distinta configuración, aplicaciones y otras reglas dependiendo de su función y perfil que se encuentra definido en la solución de gestión de identidades. Toda la configuración se aplica dinámicamente dependiendo del usuario que realice el acceso al PAN o EN. Todas las validaciones y autenticaciones se podrán hacer de forma local o verificar contra los servicios centrales.
- Sincronización y acceso a archivos. Funcionalidad para sincronizar archivos desde cualquier dispositivo que use el usuario hacia repositorios locales o hacia repositorios remotos en otros nodos NEP o en el centro de datos principal. Además de lo anterior, los usuarios pueden acceder a sus archivos personales o de carpetas compartidas desde cualquier dispositivo, ya sea virtual o de escritorio.
- Gestión de impresión. Funcionalidad para conectar cualquier dispositivo de cualquier sistema operativo hacia cualquier impresora, sin importar marca, conectada a la red.
- Gestión de archivos y carpetas compartidas. Funcionalidad para administración de carpetas compartidas y de gestión de los servidores de archivo. Debe detectar cualquier cambio o evento en el directorio institucional y lanzar tareas de creación, movimiento, borrado, cuarentena o aplicar permisos a archivos o carpetas; así como archivos con extensiones no deseadas y dejarlos en cuarentena de forma automática. Deberá poder crear espacios de almacenamiento de forma automática.
- Autenticación para escritorios de nube. Funcionalidad para que un usuario pueda acceder a múltiples sistemas o aplicaciones a través de las credenciales de autenticación por medio que el Instituto incorporó (AD).

La implementación de cada escritorio en la nube con las características antes descritas será devengada por evento por cada implementación por lo que **KIO NETWORKS** presentará una propuesta de precio para este servicio. El soporte posterior a la implementación será devengado con el Servicio de Gestión y Soporte del NEP que abarca lo definido en secciones técnicas como plataforma de nodo de extensión de nube privada.

Las implementaciones posteriores a este plan se realizarán por requerimiento y se acordará el tiempo de atención con la respuesta formal a la solicitud inicial por medio de la herramienta de gestión de servicios de **KIO NETWORKS**.

Por cada escritorio en la nube se entregará una identidad asignada a un usuario específico.

En caso de que se requieran identidades que no estén asociadas a un EN ni a los PAN, éstas tendrán un costo adicional por implementación, por lo que **KIO NETWORKS** presentará la propuesta de precio para

este servicio de "Usuario de Acceso a la Nube Privada" (UANP), y garantizará la capacidad de integración de dispositivos diferentes a PAN usando dicha identidad

4.3.3.2.5 Caché de servicios de la Nube Privada

KIO NETWORKS implementará en cada nodo de Extensión de Nube Privada, un caché de servicios de la Nube IMSS que reduzca el consumo de ancho de banda WAN, carga de los servicios alojados en el centro de datos primario, mejorar el tiempo de respuesta de las soluciones comparado con el tiempo de respuesta obtenido desde el centro de datos primario, y habilitar la disponibilidad de operación fuera de línea para los servicios y soluciones del Instituto que incorporen esa característica.

El caché de servicios de la Nube Privada formará parte de la plataforma como servicio Extensión de Nube Privada en cada nodo implementado e integrará funcionalidad de los componentes de la Nube IMSS, los cuales se describen a continuación de manera referencial:

- Notaría
- Gestor de flujo

La integración a este caché de soluciones, servicios o componentes deberán contar con la aprobación del Grupo de Gobierno del Contrato y el Área de Arquitectura del Instituto.

Cada integración será devengada por evento, previa aprobación por el Instituto, por lo que **KIO NETWORKS** hará una propuesta para este servicio. Para cada integración **KIO NETWORKS** presentará un plan de trabajo que será aprobado por el Instituto.

4.3.3.2.6 Funcionalidades generales del servicio

KIO NETWORKS proporciona una política de uso aceptable acordada con el Instituto, que prohíbe el uso de sus servicios para distribuir o almacenar material que sea inapropiado (incluyendo juegos de apuesta en línea), o material que sea ilegal, difamatorio, calumnioso, indecente, obsceno, pornográfico, no permitiendo los juegos de apuesta.

Se cuenta con una arquitectura distribuida que resida en múltiples redes dentro de diversos proveedores de servicio, asegurando con ello que no exista un punto único de fallo.

ANEXOS
DIVISIÓN DE CONTRATOS

a la Nube (PAN) y 1,200 Escritorios en la Nube (EN), igualmente deberá prever una capacidad de hasta 1000 PANs y 2000 ENs.

A continuación, se enlistan las actividades a realizar en sitio por el personal de soporte:

- Plan de mantenimiento a los puntos de acceso y periféricos cada 6 meses
- Revisión de fallas físicas
- Configuración de los puntos de acceso
- Reemplazo de piezas
- Instalación
- Reubicación física

El conjunto de personas asignadas a la gestión y soporte de los nodos de ENP serán distintos a los del Centro de Continuidad Operativa y tienen un cargo mensual por nodo de ENP, mismo que se comenzó a devengar una vez aceptada la implementación del nodo de ENP en cada ubicación.

4.3.3.2.3 Puntos de acceso a la nube

Los Puntos de Acceso a la Nube (PAN) son estaciones de trabajo ligeras que se implementaron bajo demanda y permiten el acceso a los servicios de la Nube IMSS, en especial a los EN, así como a la red del Instituto. Los PAN permiten el acceso a uno o varios usuarios (no simultáneo), por medio de identificación que determine el Instituto, teniendo separación de sus perfiles y sin estar estrechamente dependiente el punto de acceso a la nube con un usuario. Estos puntos de acceso son el medio para acceder a los escritorios en la nube, cualquier escritorio en la nube (EN) puede accederse desde cualquier PAN del nodo de ENP que pertenezca, a menos que el Instituto determine lo contrario por alguna definición de Seguridad Informática o por situaciones operativas.

Si el Instituto lo requiere, un EN es accesible desde otros nodos de ENP previo un proceso de migración del EN según lo oferte **KIO NETWORKS** para el servicio, o resguardarse en la nube indeterminadamente hasta que se requiera su acceso desde un nodo de ENP específico.

Los Puntos de Acceso a la Nube y Escritorio en la Nube serán implementados por **KIO NETWORKS** en los inmuebles que se encuentran en la cobertura de las redes locales LAN de aquellos inmuebles y campus del Nodo de ENP. Actualmente la infraestructura correspondiente a dichas redes se encuentra operativa en al menos las ubicaciones señaladas en el Apéndice "2. Ubicaciones Geográficas", por lo que **KIO NETWORKS** puede hacer uso de las mismas para proveer sus servicios, en estos casos el mantenimiento de las mismas está a cargo de **KIO NETWORKS** durante el periodo de uso de las redes que correspondan a cada uno de los PAN. En caso de ser necesario y que el Instituto lo autorice, se podrán realizar actividades de adecuación conforme al consumo de BCFs ofertados bajo la modalidad de "Integración a la Nube Privada".

Ambos elementos implementan las siguientes capacidades:

- Movilidad intrahospitalaria del personal al no depender de un equipo virtual y no físico.
- Mejora de la experiencia del usuario al tener una sola interfaz de usuario para todas las ubicaciones.
- Optimización de costos de licenciamiento y soporte en sitio a través de la consolidación de configuraciones por perfiles bajo esquemas virtuales sobre una sola instancia de EN.
- Administración de equipos centralizada, aunque los PAN se encuentren dispersos físicamente.
- Flexibilidad y escalamiento sencillo y rápido en la integración de equipos, aplicativos y almacenamiento.
- Baja demanda de espacio físico, consumos de energía y generación de calor.

La continuidad operativa permitirá brindar servicio a 1306 PANes instaladas en CMNO las cuales brindan servicio a escritorios virtuales para soportar más de 2000 usuarios en la operación continua.

Las implementaciones posteriores a este plan se realizarán por requerimiento y el tiempo de entrega del servicio será determinado y acordado por ambas partes dentro de la respuesta del requerimiento inicial. Estos tiempos, serán adicionales a cualquier trabajo requerido para acondicionar la red LAN.

Los tiempos del plan de implementación de cambios a la red LAN, serán sumados al plan de implementación de los puntos de acceso a la nube y al plan de implementación de escritorios en la nube, según aplique el caso, para efectos de niveles de servicio de implementación.

La implementación del punto de acceso a la nube será devengada por evento por cada implementación por lo que **KIO NETWORKS** presentará una propuesta de precio para este servicio. El soporte posterior a la implementación será devengado con el servicio de Gestión y soporte del nodo de ENP.

4.3.3.2.4 Escritorio en la nube

KIO NETWORKS cuenta con servicios administrados que implementen escritorios de trabajo virtuales para clientes finales.

El escritorio cuenta con las siguientes funcionalidades como parte integral del servicio:

- Escritorio de trabajo. Construcción del escritorio que incluye los Bloques de Construcción Fundamental que el Instituto determine en forma de Bloque de Construcción Común.
- Aprovisionamiento y bóveda de identidades. Funcionalidad de sincronización de identidades desde distintas fuentes y la generación del repositorio de identidades. Con esta funcionalidad el usuario consumirá su propia identidad en los sistemas asociados y usará el portal de colaboración del NEP para que restablezca su contraseña o solicitar nuevos permisos en los aplicativos.

La infraestructura administrada soporta y concentra la información de toda la plataforma de cómputo de manera eficiente, de manera centralizada respalda la información del grueso de usuarios, se administra y monitorea de manera central con grupos de soporte en sitio para brindar el soporte personalizado a usuarios finales.

4.3.3.2.1 Infraestructura e instalaciones

KIO NETWORKS facilita elementos para implementar en las ubicaciones de los ENP, infraestructura que aloje el resto de los componentes del nodo de forma segura y confiable. Las características mínimas que se cumplen actualmente por **KIO NETWORKS** son las que a continuación se describen de manera enunciativa más no limitativa:

- Sistema de control de acceso
- Nivel de disponibilidad mínimo del 99.982%
- Un sistema de redundancia eléctrica para soportar condiciones de fallo en el suministro de energía eléctrica desde la línea principal.
- Aires acondicionados de precisión en configuración N+1, todos con microprocesador inteligente que administra la temperatura y humedad relativa de la sección climatizada,
- Gabinetes de 600mm de ancho, 1000mm de profundidad y 42 RMS para instalar infraestructura de los bloques de construcción.
    - Cada gabinete contará con un sistema de rodamientos y rieles.
    - Cada gabinete contará con dos organizadores flexibles para cables.
    - Dos niveles de bandejas tipo escalerilla instaladas de manera perpendicular sobre la parte superior de los gabinetes. Una bandeja para cableado de datos y otra para cableado de potencia.
        - Un sistema de detección temprana de humo
        - Un sistema de protección contra incendios
    - Un panel de control
    - Estaciones de aborto
    - Al menos 2 sirenas/luces estroboscópicas
    - Recipientes de agente aerosol
    - Un dispositivo de grabación de video vigilancia (CCTV)
    - Al menos cuatro cámaras de alta resolución (2 internas y 2 externas)
    - Paredes internas con tratamiento de aislante térmico y acústico de material poliuretano
    - Iluminación LED.
    - Implementación de protección balística ofertada por KIO NETWORKS.
    - Un centro de conexiones eléctricas y entrada de Fibra Óptica.
    - Sistema de energía ininterrumpible (UPS) redundante.

El servicio está soportado por toda la obra civil, acometidas, permisos, traslados, herramientas, materiales, personal, así como todo lo necesario para la correcta operación. **KIO NETWORKS** mantendrá de manera eficiente cada nodo instalado dentro de las instalaciones del centro médico nacional de occidente como parte de la continuidad operativa.

KIO NETWORKS gestionará a través del coordinador la continuidad de servicio de cada nodo y es quién realizará al menos las siguientes actividades:

- Ser el enlace con el Instituto.
- Elabora y da seguimiento a la operación
- Informar de avances, riesgos y temas por resolver
- Realizar las gestiones que requiera el servicio

El Instituto continúa siendo responsable de las instalaciones donde se resguarda el centro de datos del nodo de extensión de nube privada. Para soportar la conectividad al sitio central se mantiene un enlace operativo de alta capacidad de tal forma que se interconecta a punto neutro con las garantías de alta disponibilidad y ancho de banda para soportar la operación de manera adecuada.

Las soluciones tecnológicas que forman parte integral de la plataforma de Extensión de Nube Privada son aquellas que se implementen para:

1. La relativa a la administración y operación del nodo de ENP
2. La gestión y soporte
3. Plataforma para permitir el despliegue de puntos de acceso y escritorio en la nube
4. Portal de colaboración
5. Caché de servicios de nube privada

Adicionalmente, en los nodos de ENP fueron aprovisionados como Bloques de Construcción Fundamentales descritos en el apéndice "1. Bloques de Construcción" para lo cual **KIO NETWORKS** ofertará costos específicos para esta modalidad de despliegue. La red LAN dentro de las instalaciones del nodo, y deberá respetar los estándares de interconexión, así como presentará flexibilidad en la integración a tecnología legacy de cualquier marca bajo protocolos estándares.

4.3.3.2.2 Servicio de gestión y soporte a la ENP

KIO NETWORKS proporcionará todos los elementos necesarios como herramientas, personal, hardware y software para la gestión de los servicios que se entregan en los nodos de ENP. Del mismo modo, proporciona todo lo necesario para el soporte y operación del nodo de ENP, así como los puntos de acceso a la nube y portal de colaboración.

El soporte se proporciona en sitio para los Puntos de Acceso a la Nube cuando así se requiera para lo cual, **KIO NETWORKS** mantendrá el modelo de operación actual con los recursos y horarios ya establecidos para los 4 hospitales. Cada ENP es capaz de soportar cuanto menos 400 Puntos de Acceso

ANEXO

DIVISIÓN DE CONTRA

4.3.3.1.1.5 Unidad de Conectividad de Internet. (UCI).

Proveerá conectividad hacia los servicios web nacionales y mundiales.

Considerará e incluirá todas las medidas de seguridad perimetral, así como los componentes necesarios que permitan realizar una navegación Web segura, íntegra, confiable, estable y rápida.

Tendrá la flexibilidad para soportar crecimiento en Ancho de Banda en múltiplos de 10, 20,100 y 200 Mbps hasta un máximo de 10Gbps.

Dentro de la infraestructura del servicio de Internet se deberán considerar los siguientes elementos:

- Enlaces limpios (Clean Pipes),
- ingeniería de tráfico que contemple la administración y modelado de ancho de banda en el medio de transmisión.

4.3.3.1.1.6 Unidad de Incremento de Conectividad de Internet. (UICI).

- Capacidad de conectar diferentes enlaces de Internet con capacidad de recibir todas las tablas de ruteo en una interface de 1 Gbps con incrementales de 1Gbps y hasta 10 Gbps.
- Los incrementos de los enlaces físicos de Internet tendrán que ser en interfaces de Gbps, óptico o en cobre.
- La configuración inicial de la interfaz física a Gbps será de 100 Mbps.
- Los aumentos de ancho de banda serán de manera lógica con limitación de ancho de banda en múltiplos de 100 Mbps hasta llegar a 10 Gbps.

4.3.3.1.2 Comunicaciones

4.3.3.1.2.1 Anchos de banda

Los servicios actuales atienden las solicitudes del Instituto con respecto a incrementos y/o decrementos en múltiplos de 10, 20, 100 y 200 Mbps en el Ancho de Banda, hasta un límite máximo de 10 Gbps para cualquier tipo de enlace que forme parte de los servicios solicitados en el presente anexo.

Constantemente se brinda el servicio de visibilidad donde se realiza el monitoreo de forma continua del uso de los recursos de red (por ejemplo, anchos de banda, disponibilidad, paquetes perdidos, etc.) para asegurar el nivel de servicio acordado.

KIO Networks, en conjunto con el IMSS, define las reglas de uso de los recursos y umbrales que servirán como referencia para disparar el crecimiento de las facilidades y capacidades de los enlaces con base a los reportes y notificaciones de capacidad.

En el servicio de visibilidad actual se envían mensajes cortos y/o correo electrónico al IMSS, de forma que se pueda decidir sobre el incremento de capacidad en los sitios en donde se haya excedido los umbrales.

4.3.3.1.2.2 Conectividad

Actualmente suministramos los diferentes componentes habilitadores como son enlaces y redes que permitan transportar a través de ellos de uno a otro u otros sitios paquetes de datos, video y voz, así como también incluirá el equipamiento requerido de comunicaciones, seguridad y los insumos

Estamos alineados y apegados a los estándares de comunicaciones y seguridad, así como a las mejores prácticas de la industria que garanticen técnicamente la confidencialidad, disponibilidad e integridad de los datos o información que se trasmitirá a través de los enlaces o redes que proporcione al Instituto.

4.3.3.2 Nodo de Extensión de Nube Privada

El servicio de Extensión de Nube Privada es una modalidad de despliegue de los servicios de la presente Propuesta Técnica. Se aprovisiona de manera integral como plataforma para otorgar los servicios digitales avanzados para unidades médico-administrativas. Los servicios facilitan la replicación de servicios e información, y resiliencia a errores que se refiere a la capacidad de permitir a las unidades asignadas al nodo, continuar funcionando con un conjunto específico de sistemas e información de forma local, aunque el sitio principal del IMSS u otro punto de gestión central haya quedado sin servicio.

El nodo de Extensión de Nube Privada (ENP) tiene la capacidad de implementar acceso, seguridad, gestión y archivos, usar métodos de sincronización, conectividad o federación para conectarse con el centro de datos principal. Reduce el flujo de tráfico por la WAN entre el nodo de ENP y el centro de datos principal, aumentar la disponibilidad y mejorar la respuesta en sitios de mayor relevancia y demanda de la atención de servicios digitales y de información del Instituto.

KIO NETWORKS proporcionará el servicio de ENP bajo demanda en la modalidad de plataforma, proporcionando los siguientes elementos:

- Infraestructura e instalaciones
- Gestión y soporte
- Portal de colaboración
- Puntos de acceso a la nube
- Escritorio en la nube
- Caché de servicios de nube privada

Este conjunto de elementos que conforman la plataforma como servicio ENP, es provista bajo demanda, la demanda inicial aprovisiona el nodo ENP en la ciudad de Guadalajara aprovisionando un centro de datos móvil soportando la operación del Centro Médico Nacional de Occidente.

Unidad Incremental de Conectividad MPLS (UCMPLS)

Actualmente contamos con la flexibilidad de incrementar o decrementar el Ancho de Banda a solicitud del Instituto.

Los incrementos de Ancho de Banda se llevarán a cabo en múltiplos de 10, 20, 100 y 200 Mbps hasta un límite máximo de 10 Gbps, considerando que el crecimiento de anchos de banda y escalabilidad se lleve a cabo en línea y sin disrupción.

4.3.3.1.1.2 Unidad de Conectividad Enlaces Dedicados (UCED).

Esta unidad de servicio tiene variantes por lo que su integración se fundamenta en los acuerdos que se establezcan bajo la demanda del Instituto.

Este tipo de Enlace corresponde a un enlace MPLS el cual fue definido previamente en el presente anexo.

4.3.3.1.1.3 Enlaces "LAN to LAN".

Actualmente contamos con servicios de enlace LAN to LAN (L2L) los cuales brindan una extensión del direccionamiento LAN del sitio del Instituto que se trate, hacia el sitio que el Instituto defina. Lo anterior con el fin de mantener el mismo dominio de "broadcast" mediante un enlace Ethernet. Las interfaces pueden ser de fibra óptica o cobre.

Las características que deben cubrir este servicio son:

- Interfaces físicas en cobre (RJ45) u ópticas (Conectores LC-LC) a velocidad al menos de 1 Gbps.
- Interface óptica con fibra Multimodo a velocidad al menos 1 Gbps y hasta 10 Gbps.
- Infraestructura de comunicaciones en alta disponibilidad.
- Direccionamiento IP privado con la validación del Instituto.
- Capacidad de conectar al menos 1 (un) enlace "LAN to LAN" en múltiplos de 10, 20, 100 y 200 Mbps, en el Ancho de Banda hasta un límite máximo de 10 Gbps. Fácil crecimiento de anchos de banda y escalabilidad en línea o sin disrupción.
- Monitoreo de red y análisis de tráfico.
- Infraestructura dedicada.
- El apego a las políticas de acceso físicas al Punto Neutro, serán las estipuladas por KIO Networks en acuerdo con el Instituto.
- Los enlaces se reciben en una capa extra de seguridad por medio de un clúster de firewalls que permita realizar la separación y protección de datos en la capa perimetral previo al ingreso de tráfico hacia el centro de datos, mediante políticas de "firewall", tomando en cuenta los requerimientos que la División de Seguridad Informática del Instituto determine.

Unidad Incremental de Conectividad Enlaces Dedicados (UCED).

- El Prestador de Servicios contará con la flexibilidad de incrementar o decrementar el Ancho de Banda a solicitud del Instituto.
- Los incrementos de Ancho de Banda se llevarán a cabo en múltiplos de 10, 20, 100 y 200 Mbps hasta un límite máximo de 10 Gbps, considerando que el crecimiento de anchos de banda y escalabilidad se lleve a cabo en línea y sin disrupción.

4.3.3.1.1.4 Unidad de Conectividad segura vía Internet (UCVPNI).

Conexiones a sitios remotos (Site to Site)

Definición: Son las conexiones que se hacen vía internet de forma segura utilizando hardware dedicado como Routers, Firewalls o UTMs en los inmuebles remotos con el fin de encriptar el tráfico de la red local. Para asegurar los datos se utiliza el protocolo IPSEC como protocolo estándar de la industria. Este tipo de enlaces está sujeto al SLA del ISP que da el servicio en el inmueble remoto y no en el Punto Neutro.

Las características que deben cubrir este servicio son:

- Interfaces Físicas RJ45 en cobre a velocidad de 1Gbps y hasta 10Gbps
- Interface óptica con fibra Multimodo o interface de cobre con UTP cat6A a velocidad de Gbps.
- Infraestructura de comunicaciones y seguridad en esquemas single-instance o high avalability
- Capacidad de conectar múltiples Puntos a Punto mediante tecnologías seguras y con equipos Routers, Firewalls o UTMS de diferentes marcas. En incrementales bajo demanda con dispositivos de diversas capacidades según el volúmen y requerimiento específico.
- Arquitectura de Red Hub and Spoke
- Monitoreo de red, túneles y análisis de tráfico
- Niveles de servicio 99.982%.
- Infraestructura dedicada en cajas Firewalls en modo "clúster" para los componentes centrales en punto neutro.
- Capacidad de configurar protocolos de ruteo dinámico para lograr redundancia automática de los túneles con algún otro tipo de enlace que llegue en los inmuebles de la contratante.
- Alineación de los servicios con las políticas de seguridad del Instituto.
- El apego a las políticas de acceso físicas al Punto Neutro, serán las estipuladas por KIO NETWORKS en conjunto con el Instituto.
- El centro de operaciones de red y seguridad de KIO NETWORKS realizará actividades de administración de los sistemas de seguridad, incluyendo el soporte técnico, monitoreo, manejo de incidentes de seguridad y administración de la configuración (altas, bajas y cambios), en un horario de 7 días de la semana x 24 horas al día x 365 días del año.

Unidad de Incremento de Conectividad VPN segura vía Internet (UICVPNI).

- El incremento de este servicio será en bloques de 50 sitios a conectar vía VPN's a Punto Neutro, mediante túneles de IPSec y con equipos firewalls o UTMS de diferentes marcas.

ANEXOS

DIVISIÓN DE CONTRATOS

El Servicio de Punto Neutro provee capacidades seguras de los puntos de interconexión, así como para la conectividad con los distintos tipos de redes, según se defina por los Servicios de Seguridad de la Nube IMSS.

4.3.3.1.1 Servicio de Conectividad del Punto Neutro

El Punto Neutro cuenta con la capacidad de conectividad hacia otras redes o nubes públicas que utiliza el Instituto para dar comunicación a sus inmuebles a nivel nacional, con distintos niveles de criticidad.

La implementación de cada conectividad de una nube privada hacia el Punto Neutro tiene un cargo por implementación realizada y será devengado una vez que haya sido aceptado por el Instituto de acuerdo con los criterios establecidos en el presente Anexo Técnico.

A continuación, se definen las distintas conectividades y las características que se cumplen actualmente.

4.3.3.1.1.1 Unidad de Conectividad MPLS (UCMPLS)

Redes MPLS

Son las redes de área amplia privadas para proveer servicios de telecomunicaciones. De acuerdo con las necesidades de conectividad del Instituto, así como con las diferentes nubes, incluyendo los sitios en donde se habilitan las extensiones de nube privada.

Los enlaces son entregados en los distintos centros de datos privados, públicos o híbridos tanto principales como secundarios que determinó el Instituto incluyendo los sitios donde se habilitaron las extensiones de nube privada, en los que se solicitaron para poder transportar los datos hacia el Punto Neutro, el cual es el nodo principal de las redes Punto a Punto y Multipunto de las redes nacionales.

En específico, la red MPLS (Multiprotocol Label Switching por sus siglas en inglés), tiene como objetivo principal, transportar el tráfico entre los diferentes puntos remotos por medio de un etiquetado y "switcheo" de paquetes dentro de un "backbone" del carrier que, en su caso, proporcione los servicios, de tal forma que la comunicación es "full mesh". Por lo que se garantiza técnicamente la velocidad y eficiencia de la red para transportar los paquetes de datos, video y voz.

KIO NETWORKS brinda enlaces bajo demanda, con la tecnología MPLS (Multi-Protocol Label Switching), que solicitó el Instituto, soportando realizar funciones tales como:

Ingeniería de tráfico o administración y modelado de ancho de banda, que permita asignar prioridades, garantizar ancho de banda específico (por aplicación, protocolo, horario IP, etc.) así como utilizar el ancho de banda de manera dinámica.

Políticas de Enrutamiento (Policy Routing) para direccionar el tráfico según criterios establecidos, como: la dirección origen del paquete, el tipo de tráfico o cualquier otra información contenida en el paquete.

Clase de Servicio (CoS Class of Service), que permita identificar el tráfico de datos, de video y/o de voz.

Calidad de Servicio (QoS Quality of Service), que permita asignar colas de prioridad para garantizar la prioridad de aquellos paquetes sensibles al retardo (video y voz) de los que no lo son.

Mapa de Enrutamiento (Route Map), que permite la discriminación o desvío de tráfico específico a través de listas de acceso o listas de prefijos.

Restricción de tráfico por Listas de Acceso.

Se cuenta con los medios que permiten atender las solicitudes que formule el Instituto sobre enlaces MPLS, para que estos puedan operar bajo los siguientes tipos y características:

- Activo – Pasivo. En este esquema, un enlace se encuentra funcional (primario) y el otro está disponible (respaldo o secundario) para que, en caso de falla del primero, se conmute el tráfico hacia el de respaldo, con un tiempo de afectación mínimo. Se incluirá además el transporte, la conmutación, así como el enrutamiento de paquetes, a conveniencia o solicitud del Instituto.
- Activo – Activo. En este esquema, ambos enlaces están disponibles para el transporte de paquetes, en caso de falla de alguno de los dos el que quede disponible absorbe todo el tráfico, por lo que no existe tiempo de afectación; en estos enlaces se balancea el tráfico. Se incluye además el transporte, la conmutación, así como el enrutamiento de paquetes, a conveniencia o solicitud del Instituto.

Las características que cubre este servicio son:

- Incluye VRF (Virtual Routing and Forwarding por sus siglas en inglés)
- Para interfaces físicas en cobre, estas son 1000BaseTX RJ45 con una velocidad de 1 (un) Gbps.
- Para interfaces físicas con fibra óptica multimodo BaseSX con velocidad 1 (un) Gbps y 10 (diez) Gbps.
- Incluye Clases de Servicio (CoS) y Calidad de Servicio (QoS).
- Infraestructura de comunicaciones en alta disponibilidad.
- Direccionamiento IP privado con la validación del Instituto.
- Capacidad de conectar una Red de MPLS con un enlace central mínimo de 100 Mbps con incrementales en múltiplos de 10, 20, 100 y 200 Mbps, en el Ancho de Banda, hasta un límite máximo de 10 Gbps.
- Monitoreo de red y análisis de tráfico.
- Protocolos estándares de la Industria, ruteo estático, OSPF, BGP4
- Flexibilidad para crecimiento de anchos de Banda y escalabilidad en línea y sin disrupción.

Cuenta con la capacidad y disponibilidad de la infraestructura que permita recibir enlaces de los diferentes carrier's para soportar la conectividad requerida en el Punto Neutro.

El apego a las políticas de acceso físicas al Punto Neutro, serán las estipuladas por KIO Networks y aprobadas por el Instituto.

configuraciones de escritorio. Igualmente deberá observar las políticas institucionales de seguridad y apoyarse para estos fines en los Servicios de Seguridad de Nube IMSS si así fuera necesario.

4.3.2 Consumo de BCFs y BCCs en M3 y M5

El Servicio de Integralidad y Telecomunicaciones podrá consumir BCFs y BCCs que se encuentren disponibles para la modalidad de despliegue de nube "M3: Extensión de Nube Privada (ENP) en los puntos con mayor demanda transaccional de operación de los servicios del Instituto" y "M5: Instalaciones designadas por el Instituto" conforme a lo que se especifica en la sección Elementos comunes de los Servicios, será responsable de validar su consumo y disponibilidad valiéndose de la información del **Servicio de Continuidad y Gestión de la Operación**.

4.3.3 Plataformas de Servicios de Integralidad y Telecomunicaciones

4.3.3.1 Punto Neutro de la Nube Híbrida

El Instituto tiene un modelo de telecomunicaciones para interconectar múltiples proveedores y múltiples tecnologías, formando una red híbrida, que se convierta en el Punto Neutro de comunicaciones. De esta manera las distintas necesidades del IMSS convergen permitiendo el crecimiento de servicios de transmisión de datos sin dependencias de un solo proveedor, con un marco tecnológico de conexión estandarizada, controlada y segura entre redes permitiendo tener una latencia optimizada.

Las características del Punto Neutro son:

- Redundancia: Permite la conexión de varios puntos de acceso a Internet, a la red interna del IMSS, o de proveedores de servicios digitales, de acuerdo a los lineamientos establecidos por el IMSS, habilitando redundancia de acceso; en caso de que un enlace sufra una caída en el servicio. El Punto Neutro tiene la infraestructura necesaria para recibir a los múltiples enlaces provistos por uno o varios Proveedores.
- Confiabilidad: Está ubicado en un centro de datos remoto con un nivel TIER 4, para que permita tener la disponibilidad que este servicio requiere, es redundante en todos sus componentes
- Flexibilidad: Permite conexiones de los diferentes proveedores de enlaces de comunicaciones que requiera el IMSS, mismos que pueden ser sustituidos de acuerdo con las necesidades tecnológicas de la contratante.
- Interconectividad: El Punto Neutro es el centro de conexión de los diferentes proveedores, permitiendo el flujo de información de manera controlada entre los diferentes segmentos o redes conectadas, hacia internet, la red MPLS del IMSS, enlaces a otras dependencias de gobierno o privadas, enlaces VPN, así como servicios que puedan utilizar las diferentes aplicaciones del IMSS, como el uso de notificaciones de SMS, Voz, Web y conexiones a servicios digitales terceros

M2M o B2B, tales como banca, Administradoras de Fondos para el Retiro, otras instituciones e inclusive aplicaciones comerciales a través del protocolo IP.

- Latencia Optimizada: Al concentrar a las diferentes redes en el Punto Neutro, la latencia que existe en el tráfico de información entre ellas, se vuelve un común denominador permitiendo el control del tráfico de interconexión de manera centralizada en el centro de datos, proporcionando un canal único de alta velocidad.

El punto neutro por su naturaleza imparcial y estándar contempla una capa de red WAN y una de Internet denominada en lo futuro "WAN EDGE" e "INTERNET EDGE", respectivamente. En estas capas es donde se recibirán como su nombre lo indica, los enlaces de Internet y Enlaces o Nubes de Área Amplia de los diferentes Operadores que puedan ofrecer servicios al Instituto.

Las características que cubre este servicio son:

- Interfaces Físicas. Interface RJ45 en cobre a velocidad de 1Gbps y hasta 10Gbpss.
- Interface Ópticas a velocidad Gigabit y 10 Gigabit.
- 5 Clases de Servicio MPLS.
- Infraestructura de Comunicaciones en Alta Disponibilidad tipo "carrier class" dedicada
- Capacidad de contención de fallas, tolerancia a fallas, cambio de conmutación rápida y recuperación sin interrupciones.
- Acceso al centro de datos con doble trayectoria diferente.
- Interconexión de componentes en Malla con enlaces de alta capacidad 40Mbps y 100 Mbps.
- Capacidad de conectar hasta 25 Redes MPLS.
- Capacidad de conectar hasta 30 Enlaces L2L.
- Capacidad para recibir 2500 conexiones de VPN "site to site" en IPSEC de diferentes fabricantes de equipo.
- Capacidad para recibir 500 usuarios de VPN "client to site" en IPSEC de diferentes fabricantes de equipo.
- Monitoreo de Red y Análisis de Tráfico.
- Niveles de Servicio 99.982%.
- Protocolos estándares de la Industria OSPF, BGP4, IPV4, IPV6, MPLS.
- Fácil crecimiento de anchos de Banda y escalabilidad en línea o sin disrupción.
- Aplicación de QoS y VRFS para la capa de WAN.
- Alta disponibilidad con 3 carriers de internet para garantizar el servicio.
- Capacidad y disponibilidad de interactuar en conjunto con otro proveedor de servicios para lograr automatizar la redundancia a las comunicaciones del Instituto tanto en la capa de WAN como la de Internet.
- El apego a las políticas de acceso físicas al Punto Neutro, serán las estipuladas por **KIO NETWORKS** y acordadas con el Instituto.

ANEXO
DIVISIÓN DE CONTRA

a) Instalación, Configuración y administración de la consola de administración para la plataforma de virtualización.
b) Creación de nuevas máquinas virtuales que se necesiten por nuevas necesidades del Instituto.
c) Configurar la solución de virtualización a efecto de proporcionar de manera temporal, dinámica y sin afectar ninguna de las máquinas virtuales involucradas, capacidad extra a una o más máquinas virtuales durante un intervalo de tiempo determinado con el fin de atender procesos que requieran ocasionalmente más recursos de procesamiento y/o memoria.
d) Configurar la solución de virtualización a efecto de permitir mantenimiento a los equipos físicos, dándose de baja de manera automatizada y transparente para el data center virtual, moviendo máquinas virtuales a otros nodos activos.
e) Configurar la solución de virtualización a efecto de mantener un balanceo dinámico de los recursos de hardware asignados a una o más de las máquinas virtuales del Instituto, relocalizando máquinas virtuales en nodos con menor carga de trabajo sin sufrir afectación de ninguna clase en las mismas.
f) Configurar la solución de virtualización a efecto de prevenir interrupciones en el servicio a causa de fallas de hardware, proporcionando un ambiente de alta disponibilidad en hardware que permita localizar de manera automática y sin afectación alguna en los servicios o procesos las máquinas virtuales del Instituto en uno o más nodos activos.
g) Configurar la solución de virtualización para mover máquinas virtuales entre servidores físicos y/o sistemas de almacenamiento tipo SAN/FC, iSCSI y NFS sin la necesidad de apagar las máquinas virtuales, es decir, debe poder migrar máquinas virtuales entre máquinas físicas en línea y sin interrupción en la disponibilidad de las aplicaciones y servicios que residen sobre las máquinas virtuales.
h) El software de Virtualización debe de tener la capacidad de utilizar switches distribuidos que existan a través de dos o más hosts que pertenezcan a un clúster y a su vez se administren de forma centralizada, además los switches distribuidos deben de cumplir con los siguiente:
    - Soporte de VLANs privadas
    - Soporte de L2 Forwarding
    - Soporte de IEEE 802.1Q VLAN Trunking
    - Soporte de VLAN Segmentation

i) Configurar la solución de virtualización a efecto de realizar la virtualización de equipos físicos o la conversión de máquinas virtuales en formatos de una plataforma de virtualización a otra.
j) Configurar la solución de virtualización a efecto de realizar la instalación y actualización al software de virtualización, empleando la consola central de administración como medio de envío (deployment) de dichas instalaciones y/o actualizaciones sin necesidad de interrumpir los servicios de las máquinas virtuales.
k) Configurar la solución de virtualización a efecto de crear mensualmente, sin caer en interrupciones del servicio, imágenes de máquinas virtuales activas o inactivas a manera de respaldo o con el fin de mantener máquinas virtuales para probar actualizaciones o parches permitiendo analizar el comportamiento del sistema operativo o sus aplicaciones.

4.2.4 Servicios eventuales para la Continuidad a la Operación y Soporte

A lo largo del servicio de **Continuidad a la Operación y Soporte**, se señalan una serie de servicios que pueden ser consumidos de manera eventual. Dichos servicios serán cotizados de manera individual.

4.2.5 Servicios extendidos

Conforme a lo señalado en la sección **Elementos comunes de los Servicios**, los servicios extendidos se derivan del Servicio de Continuidad a la Operación y Soporte, así como lo relacionado a la Plataforma de Virtualización.

KIO NETWORKS entregará de manera mensual la evidencia documental que soporte las acciones referentes a este apartado relativas a: Informe de los servicios extendidos derivados del servicio de Soporte a la Continuidad Operativa e Informe de los servicios extendidos si es el caso derivados de la Plataforma de Virtualización.

4.3 SERVICIOS DE INTEGRALIDAD Y TELECOMUNICACIONES

4.3.1 Soporte para la Integralidad

4.3.1.1 Servicio de soporte de Extensión de Nube Privada

KIO NETWORKS ofrecerá un servicio de mesa de servicio que:

- Coordine las actividades de despliegue
- Atienda las solicitudes de asignación de tickets relacionados a los PANs y ENs de cada Nodo de Extensión de Nube Privada
- Coordinación de actividades de comunicaciones en la zona de atención de cada Nodo de ENP
- Coordinación de actividades de personal en sitio según se especifica para cada Nodo de ENP en la sección Nodo de Extensión de Nube Privada

Igual deberá considerar el servicio de preparación de BCCs para ENs específicos a cada necesidad de los inmuebles en los que se preste el servicio, estos BCCs podrán contener entre otras cosas plantillas de ENs con aplicativos institucionales o específicos del inmueble, aplicaciones de productividad y

4.2.1.3.2 Soporte

Será responsabilidad de **KIO NETWORKS** incluir en el servicio todos los elementos para asegurar la correcta operación, soporte y continuidad de la solución tecnológica para la entrega del servicio:

a) Soporte por parte del fabricante.
b) Actualizaciones de releases, versión y certificados
c) Parches para el producto y alertas para problemas de alto impacto y correctivos de emergencia.
d) Resolución de problemas por parte del fabricante.
e) Soporte de integración de producto y multiplataforma.
f) Acceso a documentos de conocimiento, información sobre compatibilidades.
g) Acceso a foros, comunidades, boletines y otras fuentes de información por parte del fabricante.
h) Revisión y optimización de las bases de datos de las herramientas de monitoreo.

Realizar análisis de causa-raíz sobre problemas de desempeño que puedan presentarse sobre las herramientas de la presente propuesta.

4.2.1.3.3 Proceso de Gestión de Configuraciones

La gestión de la base de datos de configuraciones (CMDB) tiene como principio registrar y mantener actualizada la información concerniente a los elementos de configuración (CI) de la infraestructura operativa que se tienen para proporcionar los servicios de la presente Propuesta Técnica. Presentar al Instituto un plan de trabajo para mantener la CMDB Actualizada como parte de las actividades de ejecución del contrato.

La solución proveerá un API (Application Programming Interface) o un desarrollo compatible en la funcionalidad para lograr la integración entre herramientas de **KIO NETWORKS** y del instituto. Esta integración debe contemplar el inventario de los componentes tecnológicos de los servicios o aplicaciones que le han sido transferidos a **KIO NETWORKS** para su soporte y operación, por lo que **KIO NETWORKS** considerará todo lo necesario para llevar a cabo dicha integración, considerando los desarrollos y herramientas necesarios para llevarlo a cabo, sin costo adicional para el Instituto.

KIO NETWORKS designará un **coordinador de configuraciones**, quien tiene las siguientes actividades:

- Asegurar la actualización de la CMDB.
- Notificar al instituto los cambios realizados.

KIO NETWORKS entregará de manera mensual el Reporte de Gestión de Configuraciones que soporte las acciones referentes a este apartado.

Aspectos generales del apartado Soluciones Tecnológicas del Centro de Continuidad Operativa

KIO NETWORKS ofrece, detallar, documentar, proporcionar, habilitar, configurar, poner a punto, operar y gestionar la operación e incluir en su propuesta todo lo necesario para dar cumplimiento al rubro de **Soluciones Tecnológicas del Centro de Continuidad Operativa** requerido por el Instituto en el

presente anexo técnico, apéndices anexos, términos y condiciones, oferta de **KIO NETWORKS** y documentación contractual.

4.2.1.4 Contraprestación del servicio

El servicio de **Continuidad a la Operación y Soporte** será devengado mensualmente previa aceptación del servicio por el Grupo de Administración del Contrato.

4.2.2 Consumo de BCFs y BCCs para el Servicio

El servicio **Continuidad a la Operación y Soporte** permitirá el consumo de todos los BCFs y BCCs en modalidad de despliegue "M1: Centro de Datos externo (Centro de Datos Primario)" igualmente se encargará del despliegue de aquellos BCFs y BCCs que correspondan a sus funciones en las modalidades de despliegue "M3: Extensión de Nube Privada (ENP) en los puntos con mayor demanda transaccional de operación de los servicios del Instituto" y "M5: Instalaciones designadas por el Instituto".

KIO NETWORKS entregará de manera mensual el **Informe de Consumo y Disponibilidad de los BCFs y BCCs** que soporte las acciones referentes a este apartado.

4.2.3 Plataformas para el Servicio de Continuidad a la Operación y Soporte

4.2.3.1 Plataforma de Virtualización en M1 (PVM1)

a) **KIO NETWORKS** suministrará las plataformas de virtualización que soporten diferentes tecnologías de virtualización en la modalidad de despliegue M1. La plataforma de virtualización ofertada por **KIO NETWORKS** permite soportar una capacidad de cómputo equivalente a 800 cores/vCPUs virtuales. Cuando dicha capacidad se agote debido al despliegue de infraestructura de cómputo virtual. LA CONVOCANTE podrá solicitar Plataformas de Virtualización adicionales estimado la misma capacidad de 800 cores/vCPUs para la entrega de servicios de procesamiento.
b) Incluye todo el software y hardware, así como licencias de software, instalación, configuración, puesta a punto, soporte, operación, administración y todo lo necesario para su correcta implementación.
c) Soporta la creación y administración de máquinas virtuales, así como la configuración de toda la solución conforme a lo requerido por el Instituto.
d) El Instituto podrá solicitar durante la vigencia del contrato servicios de virtualización solicitados para las tecnologías que tenga establecidas el Marco Tecnológico de Referencia del Instituto.

Actividades que realizará **KIO NETWORKS** como parte del servicio de plataforma de virtualización:

ANEXOS

DIVISIÓN DE CONTRATOS

e) Capacidad de despliegue de Mitigaciones en tiempo real:

a. Visibilidad en tiempo real de los eventos de la mitigación
b. Visibilidad de todas las estadísticas de las mitigaciones andando
c. Selección de detalle y configuración de cada contra-medida usando la pizarra de mitigación
d. Captura simple de paquetes de datos "crudos" directamente desde la pizarra de mitigación
e. Análisis de paquetes en tiempo real que permita lo siguiente:
   I. Depurar amenazas emergentes en tiempo real antes de aplicar contramedidas.
   II. Análisis de protocolos de red

f) Soporte de las siguientes contramedidas de Mitigación:

a. Global Exception and Black / White List
b. Zombie Removal
c. TCP SYN Authentication
d. HTTP Authentication
e. DNS Authentication (Pasivo y Activo)
f. DNS NXDOMAIN Rate Limit (para ataques de diccionario)
g. TCP Connection Reset
h. Payload Regex Filtering en HTTP
i. Baseline Enforcement
j. Rate Limiting en HTTP Request, HTTP Object, SIP Request
k. Malformed Filtering en HTTP, DNS, SIP.

g) Capacidad de tomar acciones ante diferentes eventos. Al menos debe poder tomar las siguientes acciones:

a. Bloquear el tráfico anómalo sin afectar el paso de tráfico válido.
b. Alertar al operador.

El Instituto será responsable de aportar información necesaria para la implantación del servicio, así como de dar las facilidades para las pruebas de integración. Lo anterior será propuesto por **KIO NETWORKS**.

La parametrización de la aplicación deberá trabajar con el enfoque de que, únicamente, lo explícitamente aprobado por el Instituto, es permitido.

Las alternativas de solución que **KIO NETWORKS** ofrezca al Instituto deberán tener fundamentos de posicionamiento en el Mercado, y en la evaluación de los costos se considerará los de implantación del servicio, así como los costos por los servicios y su operación, mantenimiento y soporte durante la vida del contrato.

Para el suministro de la funcionalidad arriba mencionada, el Instituto proporcionará los accesos y facilidades en los equipos a monitorear de acuerdo a las políticas de seguridad vigentes y a los alcances de los contratos correspondientes.

La solución tendrá la capacidad de colectar tráfico BGP, SNMP, Netflow, Sflow, Cflow y que a partir de este tráfico pueda identificar patrones maliciosos que potencialmente puedan afectar la disponibilidad de los servicios, así como la implantación de un monitoreo de desempeño transaccional con gran capacidad de almacenamiento, la integración de esta herramienta debe permitir la rápida y eficiente consolidación, análisis, contextualización y alertamiento con fines preventivos y reactivos de eventos que puedan afectar la disponibilidad y el desempeño de las aplicaciones del ambiente de operación de la Nube privada e híbrida IMSS.

En redes BGP, la solución tendrá la capacidad de identificar patrones de tráfico seleccionados por el administrador y redireccionarlos hacia un sistema, parte de la solución, que permita al administrador aplicar filtros de tráfico con base en su criterio para eficientar, en caso de ser necesario, el uso de ancho de banda.

Visibilidad de servicios digitales y de información

Se entenderá como visibilidad a la vigilancia del estado y desempeño de BCCs, plataformas y servicios en el presente anexo técnico.

KIO NETWORKS llevará a cabo el mapeo y vigilancia de punta a punta, esto es, deberá vigilar el estado y desempeño de cada uno de los componentes de un BCC, plataforma, servicio o solución que esté alojada en el centro de datos **ofertado por KIO NETWORKS**, tomando en cuenta la relación y dependencia de sus elementos (red, procesamiento, base de datos, almacenamiento, etcétera), así como el flujo y desempeño aplicativo. Para cada implementación de visibilidad deberá realizarse un diseño específico basado en la arquitectura de la solución.

La implementación de la visibilidad deberá cubrir como mínimo los dominios de Signos Vitales, Aplicación y Experiencia de Usuario de forma integral mediante la correlación de eventos.

KIO NETWORKS entregará de manera mensual la evidencia documental que soporte las acciones referentes a este apartado, específicamente en el documento con evidencia de la herramienta tecnológica para la visibilidad de los servicios.

Para el caso de los requerimientos puntuales sobre el acceso y terminales de visualización que incluye Hardware y Software para la entrega del servicio de monitoreo, **KIO NETWORKS** entregará de manera formal al Instituto al inicio del contrato, en las fechas acordadas en las mesas de trabajo al inicio del presente contrato.

d) Generación y entrega de reportes de tráfico, protocolo, objetos administrados con GeoIP (Regiones basadas en IP) indicando de dónde viene y hacia dónde va el tráfico que se está analizando, de la siguiente forma:

a. Tráfico por país,
b. Tráfico por región,
c. Tráfico por ciudad

e) Generación y entrega de reportes en tiempo real y en forma programada de eventos que incluyen anomalías clasificadas por niveles de severidad configurables.

f) Despliegue de todas las alertas que contenga al menos la siguiente información: hora de inicio, hora de término y tipo de alerta.

g) Búsqueda de información del tráfico monitoreado.

h) Capacidad de realizar anotaciones y clasificaciones dentro de la alerta.

i) Detección a través del monitoreo de patrones de Ataques de IPv6.

j) Representaciones gráficas de tasa de transferencia de datos, ataques, vulnerabilidades, a través del tiempo para períodos de tiempo variables al menos hasta tres años.

k) Integración con otros sistemas de gestión que el Instituto indique, mediante Interfaces de Aplicaciones de Programa (API), para la gestión de eventos y análisis de flujos de tráfico.

l) Generación de información de DNS (FQDN/RDN más requeridos), HTTP y VOIP (SIP).

m) Conexión transparente a la infraestructura del Instituto, de tal forma que no entorpezca el tráfico normal, o le sume un retardo que pueda afectar la eficiencia de la red ante los servicios sensibles.

n) La solución soportará al menos los siguientes protocolos de gestión:

a. Secure Web-based GUI.
b. CLI: Console, Telnet, SSH.
c. SNMP MIB and MIB II.
d. RADIUS.
e. Syslog.

o) Análisis y filtrado dinámicamente de al menos los siguientes ataques:

a. DNS.
b. HTTP Get flood.
c. Conexiones inactivas.

p) Capacidad de monitoreo de servicios:

a. Valor agregado en servicios VoIP (SIP), Servicios basados en TCP
b. Definición de Servicio con base en la dirección IP, Protocolo, Puerto, Firmas digitales (fingerprints).
c. Monitoreo de características de rendimiento como RTT, jitter, pérdida de paquetes e impacto a los servicios
d. Base histórica de servicios específicos de datos como códigos de respuesta en SIP, DNS, HTTP.
e. Reportes de cambios en el servicio como RTT, Throughput, Jitter

q) Detectar a través del análisis de tráfico los elementos necesarios para lograr controlar acciones que influyan en el ancho de banda de la red, eventos tales como Worms, spam y otras aplicaciones residentes en los equipos terminales, que pueden afectar el desempeño de la red o a otros usuarios.

r) La solución identificará patrones de tráfico seleccionados y redireccionarlos en redes BGP hacia un sistema que permita al administrador aplicar filtros de tráfico con base en los criterios que establezca el Instituto.

s) Tipificación y evaluación de los niveles de tráfico en la Nube privada e híbrida IMSS

Mitigación de impacto por detección de ataques

El servicio incluirá mecanismos para la mitigación de impactos adversos por detección de ataques o posibles ataques, con las siguientes características:

a) Sistema de mitigación independiente a la infraestructura actual, es decir, que no requiera módulos que se instalen en chasis existentes.

b) Interactuar con la infraestructura del Instituto de tal forma que, una vez que se detecte un ataque, éste pueda ser eliminado del tráfico en curso.

c) Analizar el tráfico y crear dinámicamente los filtros que se adapten constantemente, según las características de la zona que se esté protegiendo y el tipo de ataque detectado con el fin de poder eliminar únicamente el tráfico dañino, sin requerir para operar de modo óptimo, de un monitoreo previo del tráfico por parte del equipo de mitigación.

d) Proveer la opción de Auto Mitigación, donde el sistema hace la detección y la mitigación y que se realice en forma automática, sin intervención humana.

ANEXOS

DIVISIÓN DE CONTRATOS

a. Operativas. Vistas orientadas al personal que se encarga de vigilar el estado de salud de los BCF, BCC y servicios. Esta vista está destinado a la vigilancia del servicio por el personal de **KIO NETWORKS**.
b. Gobierno y control. Vistas para el personal de operaciones del Instituto a fin de que conozcan el estado del servicio. Esta vista también podrá ser utilizada por el área de tecnología del Instituto y de **KIO NETWORKS** para la medición interna de los Niveles de Servicio.
c. Ejecutiva. Vista que concentra el estado de todos los servicios de la presente Propuesta Técnica, las vistas serán acordadas entre **KIO NETWORKS** y el Instituto, y será responsabilidad de **KIO NETWORKS** diseñar, implementar y liberar la vista hacia el usuario.

x) **KIO NETWORKS** contemplará el desarrollo e implementación de las vistas de las aplicaciones y servicios que hoy se encuentran desplegadas en el Centro de Datos actual, debiendo efectuar el análisis, diseño, configuración e implementación, así como el soporte y mantenimiento.

y) **KIO NETWORKS** implementará herramientas que permitan medir la Experiencia de Usuario, definiendo en conjunto con el Instituto las aplicaciones y servicios que requieren esta característica de monitoreo, en las mesas de trabajo durante la vida del contrato.

z) Todas las vistas deberán poder hacer consultas históricas y Drill-Down a un nivel suficiente para entender el punto de falla en caso de un evento.

aa) El servicio contemplará el personal para participar activamente en la entrega de evidencias en tiempo real y análisis de los eventos presentados por cada nivel o capa de la solución vigilada, cuando así el Instituto lo requiera.

bb) Dado que las demandas son variables y los servicios y/o BCC pueden cambiar de bloques de construcción que los componen, así como sus relaciones; a fin de lograr la mayor certidumbre en la efectividad de las detecciones positivas o reales de eventos, la vigilancia estará en constante afinación de umbrales y sus correlaciones.

Aspectos Generales de la solución de visibilidad

Monitoreo de infraestructura

Se entenderá como monitoreo la vigilancia de la salud de los BCF de forma independiente. Dichos bloques de construcción estarán integrados a la solución de visibilidad como requisito para su liberación y aceptación. El nivel de visibilidad de los bloques de construcción base será de signos vitales de los componentes que integran el bloque de construcción y sus relaciones o dependencias con las plataformas que lo habilitan.

Análisis de flujos de tráfico

KIO NETWORKS realizará todas las actividades necesarias para que el flujo del tráfico de comunicaciones que se encuentre dentro de los objetivos de nivel de servicio establecidos en la sección de Requerimiento de Niveles de Servicio.

Para tal efecto **KIO NETWORKS** realizará las siguientes funciones que se enlistan a continuación de manera enunciativa más no limitativa:

a) Análisis de capacidades actuales de los sistemas a ser migrados, así como dimensionamiento y propuesta de infraestructura en Nube privada e híbrida IMSS.

b) Análisis, dimensionamiento y labores de coordinación de la migración de los sistemas de su ubicación original a la ubicación destino.

c) Vigilancia de los flujos de tráfico de la Nube privada e híbrida IMSS.

d) Análisis del flujo de tráfico.

e) Generación de informes y reportes.

f) Generación y ejecución de mejoras para el desempeño y disponibilidad de la Nube.

g) Gestión proactiva y reactiva de incidentes y problemas relacionados con los flujos de tráfico de la Nube privada e híbrida IMSS.

h) Mitigación de los impactos o posibles impactos adversos por vulnerabilidades detectadas.

KIO NETWORKS proporcionará, como parte del servicio, una solución que incluya todo el hardware, software y personal necesarios para la entrega del servicio, la cual será suministrada, instalada, configurada, implementada, soportada y operada por **KIO NETWORKS**. Es responsabilidad de **KIO NETWORKS** mantener actualizada las versiones, parches y configuraciones para la correcta operación de la solución.

Las características mínimas que cumplirá la solución del servicio para el presente anexo técnico se mencionan de manera enunciativa más no limitativa:

a) Sistema de gestión centralizado y que concentre la administración de monitoreo. El monitoreo deberá realizarse por solución tecnológica, los componentes y los riesgos detectados, las áreas de oportunidad detectadas, las acciones de prevención o corrección a realizar a corto plazo y las planeadas a mediano plazo, el plan de trabajo de la implementación de las correcciones propuestas, dependencias y afectaciones a considerar durante la implementación, detalle de los trabajos de la implementación de las acciones de prevención / corrección, el detalle de la implementación, los registros y bitácoras, las consideraciones futuras detectadas durante la implementación y las acciones de supervisión sugeridas con motivo de la implementación de acciones preventivas o correctivas.

b) Portales web con vistas personalizadas por grupo de interés donde se pueda monitorear el tráfico y riesgos según perfil, y que permita crear limitación de opciones del menú de cada perfil.

c) Generación y entrega de reportes de riesgos detectados y mitigaciones 'activas' y detalles de las mitigaciones anteriores. Los formatos de Reporte serán como mínimo XML, PDF, Excel y CSV.

La solución tecnológica provista por **KIO NETWORKS** para este servicio contará con las siguientes funcionalidades, listadas de manera enunciativa más no limitativa:

a) La solución que **KIO NETWORKS** empleé estará alineada a lo establecido en las mejores prácticas para la operación, basándose en orientación de gestión de servicios.

b) Por cuestiones de interoperabilidad e independencia de la plataforma monitoreada, la herramienta propuesta contemplará el monitoreo sin agentes, a excepción de los casos en los cuales se demuestre la no factibilidad de esta opción o sea una necesitad especifica de profundidad que requiera instalación de agentes, en cuyo caso **KIO NETWORKS** entregará un reporte técnico que lo sustente.

c) La herramienta de monitoreo propuesta tendrá que integrar la gestión de todos los elementos relacionados e involucrados tanto físicos como lógicos, en los servicios del Instituto, que contemple las siguientes capas enunciativas, más no limitativas:

1. capa de red,
2. capa de presentación,
3. capa de procesamiento,
4. capa de almacenamiento y;
5. capa de base de datos.

d) La solución será capaz de correlacionar eventos o fallas en el funcionamiento de los diversos elementos que componen todos los servicios del Instituto, para que, en el menor tiempo posible, el personal especializado de **KIO NETWORKS** cuente con elementos para identificar, aislar la causa raíz del evento y ejecute o sugiera acciones para su resolución.

e) El acceso para administración será mediante interfaz Web a una consola centralizada desde cualquier punto de la red del Instituto. Para lo anterior, se deberán considerar por lo menos 20 licencias de acceso de conexión e infraestructura dedicada con al menos 8 terminales de visualización (pantallas con su respectivo dispositivo de acceso que permitan visualizar las plataformas de monitoreo de los componentes, aplicaciones o servicios) para las áreas de operativas y directivas del Instituto, mismas que serán instaladas donde el Instituto requiera.

f) La solución deberá manejar roles/perfiles de usuarios para definir permisos y tipo de notificación a cada uno.

g) El sistema de monitoreo permitirá integración con las soluciones de identidad y control de acceso del Instituto.

h) Permitirá contabilizar el número de veces que llega la misma alarma o evento, con el fin de evitar duplicidades.

i) La herramienta tendrá la capacidad de funcionar en un esquema de arquitectura distribuida.

j) Tendrá la capacidad de desactivarse durante las ventanas de tiempo para mantenimiento, con el fin de no generar notificaciones ni afectar los niveles de servicio durante intervenciones planeadas.

k) Proporcionar mapas jerárquicos de la topología tomando como base el elemento observado y permitir expandirlos para mostrar su interrelación con el resto de los elementos.

l) La solución permitirá el análisis en detalle o "drill-down" desde los mapas para llegar a un elemento final determinado, haciendo clicks sucesivos dentro del mapa jerárquico. Todos los mapas deben proveer de un mecanismo de "regreso" a la capa superior de la que se proviene en dicho drill-down.

m) La solución propuesta tendrá la capacidad de monitorear, filtrar, correlacionar y responder a eventos generados a partir de dispositivos de red, servidores, aplicaciones y equipos de almacenamiento.

n) La solución contará con la capacidad de exportar la información de las alarmas a archivos de bitácora con la finalidad de que puedan ser explotadas.

o) La solución tendrá la capacidad de generar y enviar alarmas o eventos vía traps SNMP o APIs a otros sistemas.

p) La solución tendrá la capacidad automática de generar y enviar alarmas o eventos a otros sistemas o dispositivos electrónicos móviles.

q) La solución será capaz de recibir alertas y/o notificaciones al menos por los siguientes medios o protocolos de administración:

1. Traps de SNMP,
2. Mensajes de Syslog,
3. Lectura de archivos de texto o logs,
4. Correo electrónico,
5. Micro blogs,
6. interfaces de Aplicaciones de Programa (API por sus siglas en inglés).

r) La herramienta tendrá la capacidad de programar políticas para escalar la atención de eventos que así lo requieran, así como el envío de notificaciones automatizadas vía correo electrónico. La estructura de las notificaciones y la relación de personal del Instituto, así como su frecuencia y escalamientos serán propuestos por **KIO NETWORKS**.

s) Consulta de información histórica de comportamientos y tendencias durante la vigencia del proyecto.

t) La herramienta entregará un Tablero de Control que permita tener una visión de 360 grados del servicio mostrando las capas que lo componen incluyendo aplicaciones, infraestructura y dispositivos monitoreados.

u) La solución será capaz de guardar históricos de la visibilidad al menos por 3 meses.

v) La solución contará con umbrales dinámicos determinados por el aprendizaje del comportamiento de los elementos vigilados, así como umbrales estáticos de advertencia y de alerta.

w) La solución será capaz de entregar distintas vistas de la salud, estado y desempeño de los BCF, BCC y soluciones, de acuerdo a perfiles de usuario. De manera enunciativa más no limitativa, se enlistan las posibles vistas:

ANEXOS

DIVISIÓN DE CONTE

KIO NETWORKS será responsable de identificar, desarrollar y aplicar las políticas y procedimientos apegados a las mejores prácticas de TI, con el fin de garantizar su continua operación de acuerdo con las características específicas de cada ambiente soportado, como, por ejemplo: reinicios programados, desfragmentación de almacenamiento, depuración de logs, instalación de parches y/o hotfixes, entre otros que defina el Instituto.

II. **Calendario**

KIO NETWORKS será responsable de proponer y acordar con las áreas correspondientes del Instituto, un calendario de mantenimiento preventivo de los Sistemas Operativos Windows de los ambientes soportados.

III. **Desarrollo y ejecución del Plan de Trabajo**

KIO NETWORKS será responsable de coordinar e integrar con los terceros involucrados, el plan de trabajo de instalaciones de parches y/o hotfixes, el cual será aplicado por **KIO NETWORKS** en los ambientes no administrados por otros contratos. Para tal efecto deberá desarrollar un plan de trabajo gestionado a través del proceso de control de cambios.

IV. **Instalación**

1. Identificación de procedimientos y obtención de parches, hotfixes, entre otros que defina el Instituto, de los distintos fabricantes.

a) Investigación y recomendaciones

KIO NETWORKS será responsable de identificar, relacionar y elaborar una propuesta para la instalación de parches y/o hotfixes que permita llevarlos al último nivel de actualización y/o documentar las excepciones que se encuentren, en todos los ambientes Windows soportados por **KIO NETWORKS**. Esto lo deberá realizar al menos de manera mensual y en coordinación con las publicaciones efectuadas por los distintos fabricantes y conforme a las mejores prácticas de TI.

b) Acceso y descarga de insumos

KIO NETWORKS será responsable de implementar los mecanismos necesarios y suficientes para garantizar su acceso a las herramientas que los diferentes fabricantes ponen a disposición, con el fin de revisar la documentación, identificar los requerimientos, riesgos y ventajas de la instalación y realizar la descarga de los insumos del software por instalar.

2. **Registro de parches e ingreso al Proceso de Gestión de Cambios**

KIO NETWORKS será responsable de registrar, encolar y/o subir en la herramienta correspondiente del Instituto, el paquete de software que contenga los parches y/o hotfixes a instalar, asegurando su integración con el Proceso de Gestión de Cambios.

a) **Ejecución**

Para los componentes, aplicativos y servicios de negocio en el alcance de esta Propuesta Técnica, **KIO NETWORKS**, una vez liberados los paquetes, deberá desarrollar la logística, coordinar y ejecutar la instalación de los mismos, considerando el impacto que ésta pueda tener a través de todas las capas

tecnológicas y efectuando las gestiones necesarias solicitadas por el Proceso de Gestión de Cambios. En caso de afectar la operación al instalar parches y/o hotfixes por causa de acciones u omisiones de **KIO NETWORKS**, se aplicarán las deductivas correspondientes en la Sección denominada "Penalizaciones y Deducciones al Pago" correspondiente al presente Anexo Técnico.

b) Validación de los parches y hotfixes aplicados

KIO NETWORKS será responsable de verificar la correcta aplicación de los paquetes instalados y el cliente validará la correcta funcionalidad del servicio en los ambientes soportados del Instituto, garantizando una plataforma operativa homogénea.

c) Reportes de parches instalados y procedimientos efectuados en Sistemas Operativos

KIO NETWORKS será responsable de elaborar y mantener un control de las actividades de mantenimiento a los Sistemas Operativos dentro del alcance de los servicios señalados en el presente Anexo Técnico, con el fin de asegurar su adecuado seguimiento y control.

KIO NETWORKS entregará de manera mensual la evidencia documental que soporte las acciones referentes a este apartado, consistentes en todos aquellos reportes, bitácoras, minutas y elementos electrónicos o impresos que comprueben el devengo de los servicios y cumplimiento de las obligaciones descritas en el presente anexo técnico, apéndices anexos, términos y condiciones, oferta de **KIO NETWORKS** y documentación contractual

4.2.1.2.11 Automatización de Comandos

Como parte de la Administración de **KIO NETWORKS** en los Sistemas Operativos, Bases de Datos y Middleware, **KIO NETWORKS** identificará los procesos, tareas y comandos que sean susceptibles de automatización (mediante programas, shells, scripts, etc.) para la ejecución de las acciones diarias de operación, eliminando posibles errores humanos y con ello llevar a cabo de manera eficiente la administración de los sistemas operativos.

4.2.1.2.12 Aspectos generales del apartado Gestión de Soporte a la Operación

KIO NETWORKS ofrece, detallar, documentar, proporcionar, habilitar, configurar, poner a punto, operar y gestionar la operación e incluir en su propuesta todo lo necesario para dar cumplimiento al rubro de ***Gestión de Soporte a la Operación*** requerido por el Instituto en el presente anexo técnico, apéndices anexos, términos y condiciones, oferta de **KIO NETWORKS** y documentación contractual.

4.2.1.3 Soluciones Tecnológicas del Centro de Continuidad Operativa

4.2.1.3.1 Visibilidad de los servicios

KIO NETWORKS aprovisionará, implementará, configurará, pondrá a punto, operar, administrará, soportará y mantendrá todos los elementos de software, hardware y recursos humanos necesarios, como parte integral del servicio.

KIO NETWORKS será responsable de revisar de manera continua, las versiones de los productos instalados en los diferentes ambientes soportados para dar aviso oportuno al Gobierno de Contrato de la presente Propuesta Técnica, 3 meses antes de la caducidad del producto y se puedan tomar las medidas pertinentes, con el fin de garantizar la vigencia del Sistema Operativo, Bases de Datos y Middleware utilizados por el Instituto.

KIO NETWORKS designará un **Coordinador de Licenciamiento y Versionamiento**, encargado de la gestión y seguimiento de las actividades de control y actualización de las versiones en uso, y contar con los recursos necesarios para mantener el control del licenciamiento y versionamiento en los ambientes soportados por el presente anexo técnico.

4.2.1.2.8 Afinación (Tuning)

Con un enfoque proactivo, durante la vida del proyecto y de manera periódica, **KIO NETWORKS** será responsable de identificar, analizar, proponer y ejecutar las tareas de optimización de configuraciones necesarias para el procesamiento, componentes y/o subsistemas que le permitan lograr los niveles de servicio establecidos por el Instituto. La Afinación se realizará en todos los ambientes del Instituto, a través de un plan de trabajo que será integrado, en el mes que se haya ejecutado para su seguimiento y control.

KIO NETWORKS será responsable de evaluar, analizar y corregir problemas de desempeño ocasionados por fallas del Sistema Operativo, Bases de Datos y Middleware y/o algún otro elemento de configuración de hardware o software (Middleware, Aplicaciones, entre otros que defina el Instituto) hasta donde el Sistema Operativo permite y agote su afinación.

KIO NETWORKS será responsable de la gestión y seguimiento de las actividades de las actividades de afinación y contar con los recursos necesarios dentro del alcance de este servicio.

4.2.1.2.9 Consolidación Tecnológica

Con el fin de cumplir con los objetivos de optimización de recursos, simplificación de procesos, reducción de costos y mitigación de riesgos de operación, **KIO NETWORKS** realizará un plan de trabajo con base en el inventario inicial para analizar los elementos tecnológicos actuales, evaluar alternativas y elaborar los planes de trabajo destinados a la consolidación de la infraestructura, con el fin de lograr durante la vida del contrato, una meta acordada y formalizada con el Instituto, a través del Grupo de Gobierno del Contrato para la reducción en la cantidad de procesadores utilizados respecto del inventario inicial, así como la optimización de licenciamiento, en aquellos equipos físicos que decida el cliente migrar a plataformas de virtualización.

Adicionalmente, **KIO NETWORKS** incluirá durante la vida del contrato, nuevos objetivos de consolidación tecnológica, conforme a las necesidades de operación del Instituto, mediante un plan de trabajo en paralelo al inventario inicial, para lo cual se acordarán objetivos particulares con el Instituto, a través del Grupo de Gobierno del Contrato de la presente Propuesta Técnica.

KIO NETWORKS utilizará las herramientas institucionales de Virtualización propias, así como una metodología de trabajo permita maximizar los beneficios para la organización y mitigar los riesgos identificados; hacer uso de prácticas y tecnologías líderes en el mercado; optimizar el soporte operativo y los niveles de servicio para los usuarios finales; definir e implementar la estrategia de consolidación/migración que satisfaga los requerimientos del Instituto; racionalizar el uso de aplicaciones donde sea apropiado; determinar una línea base del desempeño de la infraestructura antes y después de los esfuerzos de consolidación/migración; mantener un nivel de seguridad aceptable en todo momento durante los esfuerzos de consolidación/migración; y comunicar los resultados y avances al órgano de gobierno del contrato.

KIO NETWORKS entregará de manera mensual el ejercicio de consolidación en donde se pueda observar de manera enunciativa más no limitativa elementos tales como: Servidores físicos, capacidades de procesamiento físico, memoria física, almacenamiento asignado, servidores virtuales, procesamiento virtual, memoria virtual, clasificación (servidor web, servidor de aplicaciones, base de datos, etc.), software que utiliza el servidor virtual, licenciamiento, capacidades del host físico (subutilización, sobre utilización), etc. El Instituto en conjunto con **KIO NETWORKS** acordará el mecanismo de reporte y medición durante las mesas de trabajo iniciales.

KIO NETWORKS en conjunto con el Instituto definirá, vigilará y dará seguimiento a los esfuerzos coordinados de proveedores y áreas del Instituto en la consecución de las metas de consolidación establecidas en el presente Anexo Técnico.

La definición de acuerdos, mecanismos, integraciones de participantes y demás elementos necesarios para el ejercicio de consolidación serán responsabilidad de **KIO NETWORKS** en acuerdo y aprobación por parte del Instituto.

KIO NETWORKS será responsable y encargado de la gestión y seguimiento de las actividades de consolidación dentro del alcance de este servicio, y contar con los recursos necesarios para cumplir con las metas acordadas con el Instituto.

4.2.1.2.10 Mantenimiento de Plataformas

KIO NETWORKS será responsable de ejecutar la gestión y seguimiento de los procedimientos preventivos, actualizaciones y correcciones que se deberán instalar en los ambientes soportados, y contar con los recursos necesarios para coordinar todas las actividades de mantenimiento que se requieran en los ambientes dentro del alcance del servicio.

KIO NETWORKS con el objetivo de que los ambientes del Instituto se mantengan en las mejores condiciones operativas de seguridad y de integridad, se deberán realizar los mantenimientos e instalaciones de acuerdo con los siguientes puntos:

I. Políticas y procedimientos documentados

ANEXOS

DIVISIÓN DE CONT

integridad de los ambientes. Este plan de trabajo será revisado y aprobado por el grupo de Gobierno del Contrato y el área de Seguridad de la Información del Instituto.

b) Políticas de Seguridad Institucionales.

KIO NETWORKS será responsable de cumplir y aplicar las configuraciones y/o políticas específicas solicitadas por las áreas de Seguridad de la Información del Instituto y de coordinar y dar continuidad a los proyectos que ésta tenga en desarrollo, orientados a reducir las vulnerabilidades y disminuir los riesgos de seguridad de los ambientes. Con este fin, **KIO NETWORKS** proporcionará, a solicitud del Instituto.

d) Auditoría de archivos de historial (Log de Sistemas Operativos).

KIO NETWORKS será responsable de realizar una revisión continua de los eventos históricos almacenados en los archivos tipo "Log" para evaluar, gestionar y notificar con oportunidad sobre la detección de un riesgo en el sistema, acompañado de un plan de acción para solventarlo mediante el Proceso de Gestión de Cambios del Instituto. Asimismo, asegurará el resguardo histórico de dichos Logs por el tiempo y volumetría que sea acordado con el Instituto, tiempo que podrá ser actualizado mediante acuerdo formalizado para atender las necesidades de la operación. Adicionalmente, se tendrá que mantener un registro electrónico de los riesgos detectados y las actividades realizadas en cada uno de ellos.

En caso de impactos negativos en los ambientes del Instituto, derivados de la omisión de esta revisión, se aplicarán las deductivas correspondientes establecidas en la Sección denominada "Penalizaciones y Deducciones al Pago" correspondiente a la presente convocatoria.

e) Auditoría de cumplimiento normativo:

KIO NETWORKS será responsable de realizar una revisión continua del cumplimiento normativo de lineamientos de configuración de seguridad; mediante una herramienta para análisis de vulnerabilidades que les permita escanear los componentes de infraestructura dentro del alcance del servicio; incluyendo la funcionalidad de implementar políticas de seguridad e identificar aquellos equipos que no cumplan con las mismas; la generación y seguimiento de reportes de vulnerabilidades en diferentes formatos comunes (PDF, CSV, XLS, etc.); la clasificación de las vulnerabilidades y riesgos en varios niveles de criticidad (considerando al menos los niveles bajo, medio, alto y crítico). El resultado de los análisis de vulnerabilidades será compartido por el área de seguridad de **KIO NETWORKS** hacia el Instituto.

II. Seguridad Operacional

a) **KIO NETWORKS** administrará y garantizará que todas las cuentas de usuario generadas en los servidores se apeguen a las políticas de normatividad establecidas por el área de Seguridad del Instituto.
b) **KIO NETWORKS** implementará las herramientas y procesos que le permitan notificar al Instituto los incidentes de violación a cualquier política de seguridad, misma que deberá reportarse inmediatamente al Grupo de Gobierno del contrato y al área de Seguridad de la Información del Instituto, conforme a la Matriz de Escalamiento de la Operación del Servicio presentada como parte integral del Programa de Trabajo detallado correspondiente al servicio.

El área de Seguridad de la Información del Instituto será responsable de la definición de las políticas a que debe apegarse **KIO NETWORKS**; misma que vigilará su cumplimiento de manera aleatoria, como parte de la gestión y soporte del servicio dentro del alcance del contrato. Es importante mencionar que las actividades de vigilancia que realice **KIO NETWORKS** dentro del alcance de la presente Propuesta Técnica, se consideran un ejercicio complementario a cualquier otro servicio especializado de seguridad que se utilice en el Instituto, con el fin de contar con un mayor control y seguridad de la información.

c) **KIO NETWORKS** implementará y/o administrará las herramientas que le permitan la medición de contención y bloqueo de amenazas bajo los lineamientos que dicte el área de Seguridad de la Información del Instituto. Los lineamientos de seguridad referentes a los elementos de procesamiento serán acatados por **KIO NETWORKS**, quien estará obligado a la revisión y validación de las herramientas de seguridad necesarias. **KIO NETWORKS**, en conjunto con el Grupo de Gobierno del contrato y el área correspondiente de Seguridad de la Información, deberá observar la correcta instalación de dichas herramientas, incluso cuando estas sean instaladas por otras áreas operativas del Instituto administradas por diferentes contratos.
d) **KIO NETWORKS** acordará e informará de la caducidad o vigencia de los certificados de seguridad instalados en los ambientes soportados, 90 días naturales antes de dicho vencimiento. Para ello deberá administrar y gestionar estos certificados mediante un procedimiento acordado en conjunto con el área que el Instituto asigne o un tercero a través de ésta.
e) **KIO NETWORKS** contemplará que el Instituto podrá requerir la interacción con otros contratos de seguridad que existan durante la vida del contrato, para lo cual se establecerán acuerdos de niveles de operación (OLA's) entre los mismos para el intercambio de información o servicios.

4.2.1.2.7 Control del Licenciamiento y Versionamiento

- **Licenciamiento**

KIO NETWORKS, mantendrá un control del licenciamiento en la asignación y utilización de las licencias asignadas al Sistema Operativo. Para lo anterior el Instituto debe proporcionar un listado con la relación de licencias con las que cuenta. **KIO NETWORKS** avisará al Gobierno del Contrato 3 meses antes del vencimiento de las licencias.

- **Versionamiento**

KIO NETWORKS entregará un análisis de la situación actual de las versiones del Sistema Operativo, con el fin de identificar aquellas que estén próximas a salir o se encuentren fuera de soporte por parte de los fabricantes, permitiendo tomar acciones preventivas que garanticen la continuidad de la operación del Instituto.

Con base en el análisis entregado, **KIO NETWORKS** será responsable de la generación y seguimiento de un plan de trabajo orientado a garantizar la correcta actualización de las versiones del Sistema Operativo, Bases de Datos y Middleware dentro de los ambientes. Dicho plan será integrado en el mes que se haya actualizado y acordado con el Instituto.

c) **KIO NETWORKS** será responsable de realizar (o de brindar acceso con privilegios a un usuario autorizado) la instalación y/o configuración de productos de software adicional y/o productos de terceros que le requiera el Instituto (compiladores, bibliotecas, web servers, binarios, etc.) a nivel Sistema Operativo, Bases de Datos, Middleware y cualquier otro componente tecnológico. **KIO NETWORKS** recibirá una guía de instalación o configuración para los productos de terceros en los casos donde sea necesario.
d) En todos los casos que aplique y sea necesario, **KIO NETWORKS** considerará y aplicará configuraciones certificadas del fabricante del producto, o por un tercero certificado por éste, como parte de sus responsabilidades.

II. Reinstalación

a) **KIO NETWORKS** será responsable de la reinstalación o restauración de un ambiente entregado vía el protocolo entrega recepción hacia la operación con todos sus componentes de Software instalados cuando se diagnostique y/o se concluya una falta de alternativa de solución para solventar un incidente, problema o por una afectación al Sistema Operativo, Base de Datos, Middleware, así como a petición del Instituto indistintamente del nivel de protección de Hardware que se tenga.
b) Para cumplir con el inciso anterior, **KIO NETWORKS** gestionará la instalación del Sistema Operativo en su configuración básica que cumpla con las características necesarias para dicha restauración; y a partir de este punto, **KIO NETWORKS** continuará con las instalaciones y/o configuraciones necesarias hasta dejar el ambiente operando como se encontraba originalmente en todas sus capas, documentando todo lo anterior a través del Proceso de Gestión de Cambios.
c) **KIO NETWORKS** será responsable de establecer los mecanismos y alcances de respaldo necesarios (respaldo completo, File System, configuración, entre otros que defina el Instituto) que le permitan restaurar un servidor cuando **KIO NETWORKS** lo requiera, ya sea por un incidente, un problema u otra causa; o bien, por requerimiento del Instituto.
d) **KIO NETWORKS** será responsable de restaurar Bases de Datos que tenga bajo su administración, cuando diagnostique y/o pronuncie una falta de alternativa de solución para solventar un incidente o problema o cuando el Instituto así lo requiera, basándonos en la política de respaldo del Instituto.
e) **KIO NETWORKS** considerará y aplicará configuraciones certificadas del fabricante del producto, o por un tercero certificado por éste, como parte de sus responsabilidades.

4.2.1.2.5 Actualizaciones de Software

KIO NETWORKS será responsable de las actualizaciones a las versiones del Sistema Operativo, Bases de Datos, Middleware y cualquier componente de software necesarios para su funcionamiento, así como las configuraciones adecuadas derivadas de recomendaciones de terceros, a solicitud del Instituto o requeridas por la operación, con apego a las mejores prácticas de TI. Para los casos en las que dicha actualización deba ser ejecutada por otras áreas operativas del Instituto, **KIO NETWORKS** será responsable de validar la correcta instalación y/o actualización del Sistema Operativo, Bases de Datos, Middleware y cualquier componente de software, así como de notificar puntualmente a las áreas

correspondientes del Instituto a través del GGC, sobre cualquier riesgo o impacto negativo provocado por la instalación de otras áreas operativas o terceros involucrados.

Para lograr esto, **KIO NETWORKS** analizará, planeará y coordinará los esfuerzos de las áreas necesarias dentro de su organización, con las áreas internas del Instituto y con los terceros involucrados hasta su conclusión.

KIO NETWORKS será responsable de descargar actualizaciones de las versiones del Sistema Operativo, Bases de Datos y Middleware, con el fin de planear y ejecutar su implantación a través del Proceso de Gestión de Cambios del Instituto. En caso de no tener privilegios de descarga, **KIO NETWORKS** solicitará dichas actualizaciones a través del Grupo de Gobierno del Contrato para que le sean entregadas por otro medio para su instalación.

KIO NETWORKS realizará las actividades de coordinación, planeación, copiado, movimiento, replicación, migración, clonación y/o ejecución de la actualización de la configuración y/o restaurar la información del File System del Sistema Operativo, componentes y/o subsistemas relacionados entre los ambientes que el Instituto establezca, por requerimiento específico o a partir de la configuración que se necesite para los ambientes soportados, cumpliendo con los lineamientos del área de Seguridad de la Información donde aplique. En caso de las acciones antes mencionadas deban ser ejecutadas por otras áreas operativas o terceros involucrados, **KIO NETWORKS** en conjunto con el GGC definirán las acciones de planeación, coordinación y validación de cualquier actividad encaminada a la actualización de la configuración y/o restauración de File System de Sistema Operativo y componentes y/o subsistemas relacionados.

KIO NETWORKS será el encargado de designar responsables de la gestión y seguimiento de las actividades de instalación y/o actualización, y contar con los recursos necesarios para atender todas las actualizaciones que se requieran en los ambientes soportados.

4.2.1.2.6 Administración de la Seguridad en la Operación

Con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información, se requiere que se establezcan los siguientes niveles de seguridad por parte de **KIO NETWORKS**, sobre los ambientes dentro del alcance de la presente Propuesta Técnica y cuya implementación no afecte de forma negativa, genere conflicto, impida o limite las actividades que **KIO NETWORKS** realizará sobre los servicios tecnológicos, sin que éstos sean limitativos. Para lo anterior el Servicio de Continuidad Operativa atenderá y se apegará a lo que emita en políticas el Sistema de Gestión de Seguridad de Información del servicio de Seguridad.

I. Seguridad Lógica

a) Verificación de Controles de Seguridad.

Con base en el Sistema de Gestión de Seguridad de Información (SGSI), **KIO NETWORKS** será responsable de la generación y seguimiento de un plan de trabajo orientado a garantizar la correcta implantación de controles de seguridad comprendidos en el Sistema Operativo que garanticen la

ANEXO
DIVISIÓN DE CONTRA

4.2.1.2.3 Administración y Soporte del Middleware

El Middleware es un software intermedio que ofrece un conjunto de servicios que hacen posible el funcionamiento de las Aplicaciones (incluyendo en algunos casos, productos de replicación de datos), distribuidas sobre plataformas heterogéneas; que se sitúa entre las capas de aplicaciones y las capas inferiores como Base de Datos, Sistema Operativo y Red.

El Middleware ofrece servicios de infraestructura de software para que las Aplicaciones, puedan operar sobre una plataforma tecnológica e intercambiar datos entre éstas. Esto incluye servidores web, servidores de Aplicaciones, productos de replicación de datos, sistemas de gestión de contenido y herramientas similares utilizando tecnologías como XML, SOAP, servicios web y arquitecturas orientadas a servicios (SOA), entre otras que defina el Instituto.

Los componentes Middleware se distinguen de Aplicaciones finales y de servicios de plataformas específicas por cuatro importantes propiedades:

1. Son independientes de las Aplicaciones para las que éstas se desarrollan.
2. Se pueden ejecutar en múltiples plataformas.
3. Se encuentran distribuidos.
4. Soportan interfaces y protocolos estándar.

El alcance del servicio Middleware contempla la instalación, reinstalación, administración, soporte, configuración, puesta a punto, afinación, mantenimiento, respaldos, licenciamiento y versionamiento, actualizaciones, seguridad operacional y lógica, gestión, ejecución y documentación de la configuración de sus componentes; instalados en equipos físicos y virtuales en los ambientes dentro del alcance de este servicio y que no sean administrados por otros contratos y/o áreas operativas del Instituto.

Asimismo, **KIO NETWORKS** identificará y notificará al Instituto aquellos procesos, tareas, comandos, manuales que sean susceptibles de automatización a través de programas, shells, Scripts, etc. a fin de ejecutar acciones diarias de operación, eliminando así posibles errores humanos para llevar a cabo de manera eficiente la administración y soporte del Middleware.

A continuación, se señalan de manera enunciativa más no limitativa las actividades de administración y soporte que llevará a cabo **KIO NETWORKS** dentro del alcance del servicio.

a) Planear, organizar, dirigir y controlar las actividades necesarias que garanticen el óptimo funcionamiento del Middleware dentro del alcance de los servicios de la presente Propuesta Técnica, y a las que el Instituto determine durante el tiempo de vida del contrato; la instalación, reinstalación, administración, soporte, configuración, Tuning, mantenimiento, respaldos, apoyo al GGC de la presente Propuesta Técnica en la administración del licenciamiento provisto por los contratos vigentes del Instituto; así como su versionamiento, actualizaciones, seguridad operacional y lógica, gestión, ejecución y documentación de la configuración de sus componentes; instalados en equipos físicos y virtuales en los ambientes soportados.
b) **KIO NETWORKS** será responsable del soporte del Middleware garantizando la correcta y óptima operación del mismo, durante y a lo largo del tiempo de vida del proyecto aplicando las mejores prácticas de TI. Esto incluye la solución de incidentes, problemas y, en su caso, escalación con el soporte técnico del fabricante (soporte de tercer nivel) y las facultades que le serán otorgadas a

KIO NETWORKS para que cuente con los accesos requeridos a los sitios del fabricante del Middleware a fin de contar con información actualizada. Dichos accesos serán proporcionados por el Instituto de acuerdo con los contratos que tenga definidos con el (los) fabricante(s).

c) **KIO NETWORKS** será responsable de la atención de incidentes y problemas asociados al Middleware de los equipos dentro del alcance de este servicio, mediante el Proceso de Gestión de Incidentes y/o Gestión de Problemas establecidos en este documento.
d) **KIO NETWORKS** comunicará y coordinará a través del Proceso de Gestión de Cambios del Instituto aquellos cambios planeados en las funcionalidades, actualizaciones y mantenimientos del Middleware. **KIO NETWORKS** previamente revisará y analizará las solicitudes de cambio dentro del alcance de este servicio para dar a conocer al Instituto el impacto o posibles riesgos que dicho cambio implique con la finalidad de evaluar si procede o no su ejecución.
e) **KIO NETWORKS** será responsable de levantar los casos de soporte directamente a los diferentes fabricantes del middleware en caso de falla de producto, así como de dar el seguimiento correspondiente.
f) **KIO NETWORKS** contemplará un servicio de soporte de tercer nivel en productos Oracle, certificado por el mismo fabricante, quien llevará a cabo, entre otras actividades que defina el Instituto:
    - Levantamiento de casos de soporte con el fabricante del producto
    - La capacidad de identificar y entregar reportes de causa raíz validados por el fabricante
    - Contar con herramientas de soporte que permitan asistir en la recolección de información y evidencias técnicas más allá de la información que emita la plataforma de monitoreo permitiendo acelerar el análisis de un incidente.

g) **KIO NETWORKS** administrará de manera consistente los parámetros de configuración y afinación (Tunning) del Middleware a fin de garantizar la continuidad de la operación.
h) En los casos que sea requerido por el Instituto, **KIO NETWORKS** será responsable de la migración de Middleware a otro ambiente al que se encuentre actualmente.

4.2.1.2.4 Instalaciones de Software

I. Instalación

a) **KIO NETWORKS** será responsable de la habilitación, instalación, configuración y puesta a punto de los Sistema Operativo, Base de Datos, Middleware y cualquier otro componente tecnológico dentro del alcance del servicio de la presente Propuesta Técnica.
b) **KIO NETWORKS** participará en la planeación y coordinación de la instalación, configuración de Sistema Operativo, Bases de Datos, Middleware y cualquier otro componente tecnológico relacionado con los servicios de la presente Propuesta Técnica a través del Proceso de Gestión de Cambios. Asimismo, proveerá soporte durante el desarrollo de actividades que ejecuten las áreas operativas del Instituto o a través de terceros involucrados relacionados con los servicios de la presente Propuesta Técnica.

i) **KIO NETWORKS** realizará un análisis de la situación actual de la configuración de los servidores con el equipo sincronizador de tiempo, con la finalidad de que desarrolle, coordine, implemente y ejecute un plan de trabajo para mantener sincronizados todos los equipos del Instituto, si es necesario, deberá coordinar a las áreas internas del Instituto y a los terceros involucrados. Una vez implementado el plan de trabajo, **KIO NETWORKS** vigilará y monitoreará la correcta sincronización de los servidores conforme al tiempo.

j) **KIO NETWORKS** ejecutará scripts en los servidores, siempre y cuando sean solicitados a través del Proceso de Gestión de Cambios del Instituto. Asimismo, **KIO NETWORKS** previamente revisará y analizará dichos scripts para que dé a conocer al Comité de Aceptación de Cambios (CAB) el impacto y/o posibles riesgos que implica la ejecución de dichos scripts, lo anterior con la finalidad de evaluar si es que procede o no la ejecución de estos.

4.2.1.2.2 Administración de Base de Datos

KIO NETWORKS será responsable de la administración y soporte de las Bases de Datos, manejadores, instancias, así como el software relacionado, tales como: DB2, Oracle, SQL, PostgreSQL, mongo DB, entre otros que defina el Instituto durante la vida del contrato, en cualquiera de los ambientes soportados por el presente anexo técnico.

La administración y soporte de las Bases de Datos, manejadores, instancias y software relacionado incluye todas las actividades requeridas y/o necesarias para su correcta operación.

A continuación, se señalan de manera enunciativa más no limitativa las actividades de administración y soporte de las Bases de Datos, instancias, y software relacionado que llevará a cabo **KIO NETWORKS** dentro del alcance de los servicios de la presente Propuesta Técnica:

a) **KIO NETWORKS** será responsable de la administración, configuración y soporte de las Bases de Datos, manejador de Bases de Datos, instancias, y software relacionado.
b) **KIO NETWORKS** será responsable de realizar las altas, bajas y cambios de las Bases de Datos, los manejadores de Bases de Datos, instancias, y software relacionado a través del Proceso de Gestión de Cambios.
c) **KIO NETWORKS** será responsable de la resolución de incidentes y problemas asociados a las Bases de Datos, instancias, y software relacionado mediante los Procesos de Gestión de Incidentes y Gestión de Problemas definidos en el presente Anexo Técnico.
d) **KIO NETWORKS** comunicará y coordinará a través del Proceso de Gestión de Cambios del Instituto aquellos cambios planeados, previamente revisará y analizará las solicitudes de cambio dentro del alcance de este servicio para dar a conocer al Instituto el impacto o posibles riesgos que dicho cambio implique con la finalidad de evaluar si procede o no su ejecución. Asimismo, deberá involucrar a los diferentes grupos de Soporte (Aplicaciones, Redes, Almacenamiento, Sistemas Operativos, entre otros que defina el Instituto) y terceros involucrados.
e) Derivado de una recomendación, valoración, incidente, problema y/o propuesta de un tercero, **KIO NETWORKS** mediante las mejores prácticas será responsable de analizar, medir el impacto y riesgo operativo, desarrollar un plan de trabajo, coordinarse con terceros y ejecutar las acciones derivadas mediante el Proceso de Gestión de Cambios del Instituto.

f) **KIO NETWORKS** definirá y/o ejecutará los requerimientos de configuración del manejador de bases de datos (instancias). Asimismo, deberá coadyuvar a la tropicalización con las áreas internas y/o con los terceros involucrados; entiéndase como tropicalización la configuración adecuada del manejador con los ambientes propios del Instituto.
g) **KIO NETWORKS** ejecutará los requerimientos de homologación de configuraciones de las Bases de Datos, instancias, objetos y software relacionado para los diferentes ambientes. **KIO NETWORKS** mantendrá consistencia entre los parámetros de todas las Bases de Datos que están directamente asociados a un tamaño o plataforma cuando éstas sean similares.
h) En los casos que sea requerido por el Instituto, **KIO NETWORKS** será responsable de la migración de Bases de Datos a otro ambiente al que se encuentre actualmente y dentro del alcance de este servicio.
i) **KIO NETWORKS** instalará y proveerá las herramientas que le permitan automatizar las tareas de administración, generación, modificación, monitoreo y soporte de las Bases de Datos.
j) En caso de presentarse una falla técnica del producto en los diferentes manejadores, el soporte técnico será provisto por el fabricante siempre y cuando la versión este soportada, para lo cual el Instituto contará con los contratos de cada uno de los productos que se encuentren en operación. En caso de requerir apoyo del fabricante, **KIO NETWORKS** interactuará, escalará y coordinará con el fabricante, sí y sólo si, el producto tiene un defecto.
k) **KIO NETWORKS** se apegará al mecanismo que el fabricante tenga definido para el levantamiento de un reporte, notificando al GGC del estado del reporte.
l) **KIO NETWORKS** contemplará un servicio de soporte de tercer nivel en productos Oracle, quien llevará a cabo entre otras actividades que defina el Instituto:
    - Levantamiento de casos de soporte con el fabricante del producto.
    - La capacidad de identificar y entregar reportes de causa raíz validados por el fabricante.
    - Contar con herramientas de soporte que permitan asistir en la recolección de información y evidencias técnicas más allá de la información que emita la plataforma de monitoreo permitiendo acelerar el análisis de un incidente.
m) **KIO NETWORKS** con el fin de evitar la degradación en el rendimiento de los equipos será responsable de validar que al menos las bases de datos estén excluidas del escaneo del antivirus institucional instalado en los servidores y/o cualquier recomendación del fabricante que provoquen una degradación.
n) **KIO NETWORKS** administrará de manera consistente los parámetros de configuración del manejador de Base de Datos a fin de garantizar la continuidad de la operación.
o) **KIO NETWORKS** vigilará y mantendrá activas y vigentes las cuentas administrativas y operativas de Bases de Datos, de los ambientes soportados y bajo las políticas definidas por el servicio de gestión de seguridad de la información, dentro del alcance del servicio con el fin de evitar que éstas expiren e impacten negativamente en la operación.
p) **KIO NETWORKS** ejecutará scripts en los servidores del Instituto, siempre y cuando sean solicitados a través del Proceso de Gestión de Cambios y se tenga el visto bueno de las áreas de Seguridad de la Información del Instituto cuando así aplique. Asimismo, **KIO NETWORKS** previamente revisará y analizará los scripts para que dé a conocer al Grupo de Gobierno del Contrato el impacto o posibles riesgos que implica la ejecución de dichos scripts, lo anterior con la finalidad de evaluar si es que procede o no la ejecución de estos.

ANEXOS
DIVISIÓN DE CONTRATOS

- La Mesa de Servicio debe proporcionar el primer soporte (nivel 1) para la atención inmediatamente del ticket.
- La Mesa de Servicio debe dar seguimiento de inicio a fin para la resolución y/o atención del ticket, pasando por cualquier área de soporte dentro de los niveles: N2 y N3.
- El número de ticket se proporcionará en todos los casos a la persona que solicitó el ticket, cualquier omisión del número de ticket, se considerará como un ticket fallido.
- Todos los tickets deberán registrar el horario en que sean creados.
- Los tickets serán cerrados hasta que el incidente, evento o requerimiento, haya sido solucionado por completo y confirmado por la persona que levantó el ticket, por cualquiera de los canales que habilite la mesa, siempre y cuando genere evidencia de la confirmación del usuario.

KIO NETWORKS entregará mensualmente el **Reporte de Tickets Generados** que incluya de manera enunciativa más no limitativa lo siguiente

- Número de ticket: incidente, problema, evento, requerimiento.
- Fecha de apertura.
- Fecha de solución.
- Tiempo de solución.
- Comentarios de solución.
- Niveles de servicio de ticket.

4.2.1.2 Gestión de Soporte a la Operación

4.2.1.2.1 Administración de Sistemas Operativos

La administración de sistemas operativos contempla la gestión, instalación, configuración, actualización, mantenimiento, soporte, así como la ejecución y documentación de configuraciones de los sistemas operativos, sus componentes y/o subsistemas instalados en equipos físicos y virtuales, salvo aquellos casos que a petición del Instituto la administración del sistema operativo sea compartida con **KIO NETWORKS** durante un período de transición que se establezca por acuerdo entre ambas partes.

A continuación, se señalan de manera enunciativa más no limitativa las actividades de administración y soporte de sistemas operativos que llevará a cabo **KIO NETWORKS** dentro del alcance de los servicios de la presente Propuesta Técnica:

a) **KIO NETWORKS** será responsable de las actividades de administración de los sistemas operativos que les sean señalados y/o transferidos por parte del Instituto; considerando para dicha operación la aplicación de los procedimientos que sean necesarios para cumplir con las actividades que establece el Proceso de Administración de la Operación (AOP) del MAAGTICSI vigente; para lo cual deberá desarrollar, implementar y mantener disponibles para su consulta y actualización electrónica, los documentos, herramientas y registros que permitan verificar su cumplimiento (Ejemplo: Mecanismos de Operación, Programas de Tareas, Bitácoras de Operación, etc.).
b) **KIO NETWORKS** será responsable de la administración, configuración y soporte de los sistemas operativos componentes y/o subsistemas definidos dentro del alcance del servicio, salvo en los

casos en que deban ser gestionados de manera total o parcial por otras áreas operativas del Instituto, o por Proveedores de contratos que tenga el Instituto. **KIO NETWORKS** trabajará con el Instituto para validar la correcta administración y desempeño de dichos sistemas operativos, así como para planear y coordinar las acciones que se requiera que se ejecuten de manera conjunta.
c) **KIO NETWORKS** será responsable de la atención y/o canalización al área operativa correspondiente de los incidentes y problemas asociados a los sistemas operativos, componentes y/o subsistemas asociados de los equipos dentro del alcance del servicio mediante el Proceso de Gestión de Incidentes y/o Problemas del Instituto, alineados al MAAGTICSI vigente.
d) **KIO NETWORKS** comunicará y coordinará a través del Proceso de Gestión de Cambios del Instituto aquellos cambios planeados en las funcionalidades, actualizaciones y mantenimientos a los sistemas operativos, sus componentes y/o subsistemas. **KIO NETWORKS** previamente revisará y analizará las solicitudes de cambio dentro del alcance de este servicio para dar a conocer al Instituto (a través de la Mesa de Cambios Institucional) el impacto o posibles riesgos que dicho cambio implique con la finalidad de aportar elementos técnicos para evaluar si procede o no su ejecución.
e) **KIO NETWORKS** será responsable de levantar los casos de soporte directamente a los diferentes fabricantes del sistema operativo, sus componentes y/o subsistemas en caso de falla de producto, así como el seguimiento correspondiente. Dada la diversidad de entornos que el Instituto utiliza en su operación, **KIO NETWORKS** contará con el personal y los recursos necesarios para el registro, seguimiento y cierre de los casos de soporte con el fin de garantizar la continuidad de la operación. **KIO NETWORKS** se apegará al mecanismo que el fabricante tenga definido para el levantamiento de un reporte, actualizando el estado en el que se encuentran.
f) En los casos que sea requerido por el Instituto, **KIO NETWORKS** será responsable de la creación, conversión y/o migración de ambientes de procesamiento virtual a físico, físico a virtual o virtual a virtual, contenedores (incluyendo todos sus componentes instalados: base de datos, middleware, aplicaciones), entre cualquiera de los centros de datos que utiliza el Instituto (incluyendo servicios en la nube); mediante el uso de los diferentes componentes de software de Virtualización que defina y/o integre el Instituto, Asimismo, deberá realizar la creación y administración de plantillas (Templates) que se requieran de dichos ambientes.
g) **KIO NETWORKS** administrará de manera consistente los parámetros de configuración del sistema operativo, sus componentes y/o subsistemas, a fin de garantizar la continuidad de la operación. En los casos en los que, por disposición del Instituto éstas funciones recaigan en otras áreas operativas del Instituto, **KIO NETWORKS** tendrá la obligación de validar el correcto funcionamiento del sistema operativo y reportar al Instituto, cualquier incidente o problema que impida o limite el desempeño del sistema operativo, sus componentes y/o subsistemas. **KIO NETWORKS** dirigirá y coordinará todas las acciones de planeación y ejecución con otras áreas operativas y/o terceros que se requiera para garantizar el correcto funcionamiento del sistema operativo, sus componentes y/o subsistemas.
h) **KIO NETWORKS** vigilará y mantendrá activas y vigentes las cuentas administrativas y operativas del sistema operativo, sus componentes y/o subsistemas en los ambientes soportados y definidos dentro del alcance del servicio con el fin de evitar que éstas expiren e impacten negativamente en la operación, si esto último ocurre.

Instituto durante las mesas de planeación del arranque y que podrá modificarse durante la vigencia del contrato.

El proceso asegurará que se utilicen métodos y procedimientos estandarizados para el manejo de todos los cambios, optimizando el riesgo total del negocio y reduciendo los incidentes, interrupciones y el re-trabajo.

KIO NETWORKS categorizará los cambios en Normales, Estándar y Emergentes de acuerdo a los criterios que establezca el Instituto en su modelo operativo vigente durante la vigencia del servicio.

KIO NETWORKS planeará y organizará los cambios en grupos y secuencia a ejecutarse en días y horarios preestablecidos en común acuerdo con el Instituto, a fin de prevenir afectaciones adversas y realizar validaciones.

Todos los cambios serán registrados en la solución tecnológica que integre la herramienta del instituto con la de **KIO NETWORKS** para la gestión de servicios.

El Gestor de Cambios asegurará que los planes de cambio incluyan todos los elementos para su ejecución, así como los planes de retorno.

KIO NETWORKS designará un **Gestor de Cambios** que será el coordinador y responsable de que todos los cambios se gestionen de acuerdo al proceso que se establezca en conjunto con el Instituto. El Gestor de Cambios será en enlace con el Instituto para los cambios.

Actividades a cargo de **KIO NETWORKS**

- Asegurar que los cambios sean registrados, evaluados, autorizados, priorizados, planeados, probados, implementados, documentados y revisados de una forma controlada.
- Planear y controlar los cambios.
- Participar en la planeación.
- Medir y controlar los cambios.
- Generar información para la toma de decisiones.
- Recibir, registrar y asignar prioridad a todos los RFCs.
- Rechazar los RFC que no se encuentren completos.
- Asesorar en el llenado de los RFC.
- Promover los cambios ante el CAB del Instituto.
- Solicitar ante el ECAB la aprobación de los cambios emergentes.
- Análisis de impacto previo a la ejecución del cambio.
- Participar presencialmente en las sesiones de reuniones calendarizadas de parte del Instituto.

KIO NETWORKS entregará mensualmente el **Reporte de Gestión de Cambios** que incluya de manera enunciativa más no limitativa lo siguiente:

- Número de Requerimientos de Cambio (RFC).
- Duración del Cambio.
- Resultado del Cambio.

- Desviaciones.
- Áreas de oportunidad identificadas.
- Relación de cambios que afectan activos de TI y que deberán de ser actualizados en la CMDB

4.2.1.1.6 Mesa de Servicio

KIO NETWORKS implementará una herramienta de Mesa de Servicios para recibir, registrar, categorizar, dar seguimiento y generar información de los procesos de Gestión de Requerimientos, Gestión de Eventos, Gestión de Incidentes, Gestión de Cambios y Gestión de Problemas, relacionados a los servicios de la presente Propuesta Técnica.

A continuación, se describen de manera enunciativa más no limitativa, algunos de los eventos que se podrán reportar a la Mesa de Servicio:

- Fallas de hardware en los servidores suministrados al Instituto.
- Degradación de servicio en las aplicaciones o servicios del Instituto.
- Fallas de funcionamiento en Sistema Operativo.
- Fallas de funcionamiento en Bases de Datos.
- Fallas en el software de monitoreo.
- Fallas y/o degradación en los servicios de comunicaciones, por ejemplo, en el enlace LAN to LAN.

KIO NETWORKS categorizará y asignará en tiempo y forma los tickets solicitados por el Instituto, registrando de manera enunciativa más no limitativa:

- Nombre del solicitante.
- Cargo y/o puesto.
- Síntoma.
- Evidencia.
- Servicio afectado.
- Número y correo electrónico para validación de confidencialidad
- Grupos de soporte

KIO NETWORKS considerará todo lo necesario para llevar a cabo la integración con la Mesa de Servicios Tecnológicos del Instituto, así como los desarrollos, personal especializado y demás herramientas necesarias para llevarlo a cabo, sin costo adicional para el Instituto.

La Mesa de Servicio estará disponible para atender y gestionar los tickets en un horario de servicio 7x24x365. **KIO NETWORKS** será responsable de contar con los agentes necesarios para atender la demanda en los diferentes turnos.

Los tickets generados por la Mesa de Ayuda serán despachados hacia los grupos de soporte establecidos por categorización, cuidando en todo momento lo siguiente:

ANEXOS

KIO NETWORKS entregará mensualmente el **Reporte de Gestión de Incidentes** que incluya de manera enunciativa más no limitativa lo siguiente:

- Número de incidente.
- Fecha y hora de apertura del incidente.
- Fecha y hora de solución del incidente.
- Tiempo de solución del incidente
- Información sobre acciones de restauración, diagnóstico y solución.
- Servicio afectado.
- Recurrencia de servicios afectados
- BCFs, BCCs afectados de manera directa e indirecta.

4.2.1.1.4 Gestión de Problemas

Se considerará un Problema a una condición identificada en múltiples incidentes que exhiben síntomas comunes y de la cual no se conoce la causa raíz que originó el incidente.

KIO NETWORKS analizará y encontrar la causa raíz que ocasionan eventos e incidentes; realizar actividades proactivas para detectar y prevenir futuros incidentes y definir un subproceso de errores conocidos que permita el diagnóstico de una manera más ágil.

KIO NETWORKS registrará un nuevo problema por uno o varios incidentes recurrentes cuando no exista una solución rutinaria o bien no se conozca la causa raíz que originó la interrupción o degradación en el servicio.

Para la solución de los problemas que se presenten en los servicios descritos en el presente Anexo Técnico, **KIO NETWORKS** contará con grupos especializados para la atención y diagnóstico de los problemas, conformados por especialistas en las tecnologías descritas en el presente anexo técnico y personal del Instituto.

KIO NETWORKS designará un **Gestor de Problemas** quien se encargará de asegurar el cumplimiento del proceso.

Actividades a cargo de **KIO NETWORKS**

- Operar la solución tecnológica para la gestión de problemas.
- Gestionar la solución de problemas.
- Documentar el problema en conjunto con el Instituto.
- Generar informes del seguimiento del problema.
- Documentar el cierre del problema.

Actividades del Gestor de Problemas de KIO NETWORKS:

- Organizar, conformar y coordinar los grupos de atención de problemas.
- Ser el enlace con el Instituto para dar seguimiento e informar.
- Ser administrador y resguardar la base de conocimiento de errores conocidos.

- Realizar análisis de casos en la solución tecnológica, principalmente de incidentes y eventos, para detectar problemas.
- Dar seguimiento en la solución tecnológica y registrar errores conocidos
- Realizar el cierre formal del registro de problemas.
- Ordenar, ejecutar, documentar y dar seguimiento a las actividades relacionadas con la revisión de problemas mayores.
- Generar el plan de trabajo para resolver el problema y dar seguimiento a la ejecución de las actividades.
- Coordinar el registro de los cambios que apliquen, para resolver el problema.
- Generar los indicadores clave de desempeño que correspondan al proceso.
- Realizar el cierre formal del registro de problemas a través de un dictamen.
- Participar presencialmente en las sesiones de reuniones calendarizadas de parte del Instituto.
- Generar el **Dictamen Técnico del problema**

KIO NETWORKS entregará mensualmente el **Reporte de Gestión de Problemas** que incluya de manera enunciativa más no limitativa lo siguiente:

- Número de problema.
- Fecha de apertura del problema.
- Fecha de solución del problema.
- Cantidad de incidentes recurrentes.
- Cambios asociados al problema.
- Acciones semanales para identificar la causa raíz.
- Incidentes resueltos sin causa raíz detectada.

4.2.1.1.5 Gestión de Cambios

Se considerará un cambio normal cualquier, modificación o eliminación de servicios, elementos de configuración, procesos, documentación, bloque de construcción o relaciones entre componentes en el ecosistema Institucional. Los cambios normales deberán solicitarse mediante un Requerimiento de Cambio (Request for Change RFC) en la solución tecnológica que implemente **KIO NETWORKS** para la gestión de servicios. Los cambios normales serán sometidos a la aprobación y programación del comité de cambios (Change Advisory Board CAB) que el Instituto señale.

Un cambio estándar es un cambio pre-aprobado por el Instituto, de bajo riesgo, común y sigue un procedimiento o instrucción de trabajo específico. No se solicitarán Requerimientos de Cambios para implementar cambios estándar, pero sí serán registrados y documentados.

Un cambio emergente que será introducido lo más rápido posible previa autorización obtenida del comité de cambios de emergencia (Emergency Change Advisory Board ECAB) conformado por personal del Instituto y de **KIO NETWORKS**, solo para resolver un incidente mayor y/o un requerimiento de negocio regulatorio. Por lo anterior, un cambio emergente tendrá un procedimiento específico que definirá el

KIO NETWORKS entregará mensualmente el **Reporte de Gestión de Requerimientos** que incluya de manera enunciativa más no limitativa lo siguiente:

- Número de requerimiento.
- Fecha y hora de apertura del requerimiento.
- Fecha y hora de solución del requerimiento.
- Tiempo de solución del requerimiento.
- Información sobre acciones de restauración, diagnóstico y solución del requerimiento.

4.2.1.1.3 Gestión de Incidentes

Se considerará un "incidente" a una interrupción no planificada o reducción en la calidad de un componente, aplicación, servicio o elemento tecnológico descrito en el presente anexo técnico. También será considerado un incidente a la falla de un elemento de configuración, BCF, BCC o plataforma, aunque no haya impactado todavía en el servicio.

El proceso deberá restablecer la operación normal del servicio en caso de un incidente tan rápido como sea posible, minimizando el impacto adverso en los componerites, aplicaciones y servicios digitales soportados por el presente anexo.

El impacto y la urgencia estarán definidas en las mesas de trabajo de inicio del contrato entre **KIO NETWORKS** y el Instituto.

Para resolver los incidentes, **KIO NETWORKS** considerará las prioridades que se establezcan en base al impacto y a la urgencia.

Para la gestión de Incidentes, **KIO NETWORKS** contará personal especializado en la gestión y deberá coordinarse con los grupos de soporte y gestión que el Instituto determine durante la vida del presente contrato o quien éste señale. **KIO NETWORKS** designará un **Gestor de Incidentes** quien supervisará el apego al proceso de Gestión de Incidentes, y realizará de acuerdo con este proceso, sugerencias de mejora.

Será considerado un **Incidente Mayor** aquel que deja fuera de operación al menos un servicio crítico del Instituto, algún BCF o BCC que afecte de manera colateral otros servicios o aplicaciones del Instituto, BCF o BCC considerados transversales, Fallas masivas de red, o cualquier servicio que el Instituto haga de conocimiento a **KIO NETWORKS**. **KIO NETWORKS** establecerá, en conjunto con el Instituto, el procedimiento especial para la atención de **Incidentes Mayores** y apegarse a la normatividad vigente del Instituto, que incluya al menos de manera enunciativa más no limitativa: mecanismos de notificación, mecanismos de comunicación, matrices de escalación, grupos de soporte y mesas de trabajo especializadas para la atención de incidentes (WarRooms).

KIO NETWORKS definirá los grupos de soporte establecidos y especializados de primer, segundo y tercer nivel de atención.

KIO NETWORKS se apegará a los niveles de escalamiento que se definan en conjunto con el Instituto en las mesas de trabajo durante la vigencia del contrato.

KIO NETWORKS habilitará mecanismos de comunicación agiles (foros sociales, herramientas móviles de comunicación, etc.) para el seguimiento de **incidentes (incluyendo los mayores)**, e informar en un resumen final por mecanismos de comunicación formales que el Instituto acuerde con **KIO NETWORKS** (correo electrónico, post-mortem, etc.) el resultado de las acciones de solución del Incidente. Estos mecanismos de comunicación formales y agiles, estarán aprobados, administrados y supervisados en conjunto con el Instituto y **KIO NETWORKS**.

KIO NETWORKS entregará, en un plazo no mayor a 72 horas posterior a la solución del incidente, un reporte de análisis **"post-mortem"** de los **incidentes mayores**, o aquellos que el Instituto solicite, así como la propuesta de cálculo de deductiva o penalización por incumplimiento de niveles de servicio, que incluya todos los BCFs y BCCs afectados de manera directa e indirecta. En los reportes post mortem, **KIO NETWORKS** entregará al menos de manera enunciativa más no limitativa:

- Cronología del Incidente desde su detección, notificación, acciones, grupos participantes, hasta su solución.
- Lista de BCFs, BCCs, afectados de manera directa.
- Componentes, aplicaciones, o servicios afectados colateralmente desglosados en BCFs y BCCs.
- Duración del incidente (detallado por BCF y BCC afectado).
- Acciones de mejora o recomendaciones.

Para la gestión de Incidentes **KIO NETWORKS** efectuará de manera enunciativa más no limitativa, las actividades siguientes:

- Operar la solución tecnológica para la gestión de incidentes.
- Identificar y registrar los incidentes.
- Categorizar, priorizar y realizar diagnóstico inicial.
- Investigar y diagnosticar.
- Solucionar y recuperar.
- Cerrar el incidente.
- Informar al Instituto el estado de los incidentes.

Actividades del Gestor de Incidentes de KIO NETWORKS:

- Gestionar el Incidente en conjunto con el Instituto.
- Desarrollar e implementar el proceso.
- Vigilar el cumplimiento y apego al proceso.
- Realizar ajustes y actualizaciones al proceso.
- Desarrollar los indicadores clave de desempeño (KPIs)
- Gestionar el desarrollo de los reportes de indicadores.
- Participar presencialmente en las sesiones de reuniones calendarizadas de parte del Instituto.
- Elaborar el reporte postmortem.
- Entregar propuesta de penalización o deductiva.
- Abrir los canales de comunicación necesarios para la atención de incidentes (brigdas telefónicos, foros de comunicación ágil, foros móviles etc.).

ANEXOS
DIVISIÓN

4.2.1.1.1 Gestión de Eventos

Se entenderá como "evento" todo cambio de estado significativo de un elemento de configuración, BCF, BCC o componente tecnológico, que pueda afectar de manera negativa la prestación del servicio al Instituto, en términos de degradación, desempeño o inclusive denegación.

KIO NETWORKS establecerá los mecanismos necesarios para detectar eventos que ocurran en los BCFs, BCCs y en cualquier componente tecnológico, su interpretación, notificación y acciones de control que apliquen para su recuperación, así mismo, los eventos podrán indicar que alguna aplicación, servicio o componente no está funcionando correctamente mediante el registro de un incidente a través del proceso descrito más adelante; también pueden indicar una actividad anormal, o la necesidad de una intervención de rutina. Además de indicar el alcance de umbrales operativos.

Los eventos deberán comunicar información operacional a otros procesos de gestión como incidentes, cambios y problemas.

La gestión de eventos deberá operar en un horario 7x24x365 a partir de su implementación y hasta el término del Contrato. Para tal efecto **KIO NETWORKS** considerará la cantidad de estaciones (agentes más terminales de monitoreo) necesarias para cubrir el horario antes definido.

Este servicio tiene como objetivo conocer la salud de los BCF y los BCC de los servicios tecnológicos asociados al presente anexo técnico, mismo que deberán dar visibilidad al equipo que gestiona el servicio de parte del Instituto.

El servicio deberá hacer énfasis en todo momento a la proactividad, es decir, tendrá la capacidad de poder identificar anticipadamente una posible falla en cualquiera de los componentes de los bloques de construcción o servicios de la presente Propuesta Técnica, notificando mediante alertas a las áreas correspondientes para que se tomen acciones antes de que un evento se materialice en un incidente.

KIO NETWORKS en el monitoreo proactivo considerará, la identificación de los BCF, métricas adecuadas para cada bloque de construcción en el contexto de su implementación, la definición de los umbrales óptimos y sus correlaciones, de alerta y críticos de operación de cada uno de ellos, el seguimiento permanente de los mismos y los esquemas de escalamiento y seguimiento que correspondan a la acción y atención preventiva con el Instituto o los grupos de soporte definidos en las mesas de arranque.

KIO NETWORKS designará un **Coordinador de Eventos,** con los conocimientos y la experiencia necesaria para la administración y seguimiento de este servicio.

KIO NETWORKS como parte de la gestión de eventos, implementará a través de herramientas tecnológicas, la visibilidad a los componentes de la infraestructura, como son los signos vitales (CPU, memoria y acceso a disco), BCF's, BCC y sobre todo las afectaciones colaterales por la degradación del componente, aplicativo o servicio, informando de manera oportuna al Instituto sobre su gestión.

El servicio tendrá la visibilidad de todos los elementos de configuración (CIs) que formen parte del ecosistema de los servicios que sean transferidos hacia **KIO NETWORKS**, los cuales estarán relacionados de manera ordenada en la **CMDB**.

Actividades enunciativas más no limitativas a cargo de **KIO NETWORKS:**

- Operar la solución tecnológica que permita la visibilidad de los componentes y servicios.
- Detección y filtrado de eventos.
- Registro de eventos en la solución tecnológica
- Correlacionar y dar significado a los eventos
- Seleccionar respuesta y acciones a realizar
- Consultar la Base de Conocimiento
- Acciones de revisión de los componentes y servicios
- Registro de Incidentes por alertamiento de los eventos materializados impactando el servicio.
- Cerrar evento.
- Participar presencialmente en las sesiones de reuniones calendarizadas de parte del Instituto.
- Identificar afectaciones colaterales en servicios que ocupen el componente, aplicación o servicio afectado.

KIO NETWORKS entregará mensualmente el **Reporte de Gestión de Eventos** que incluya de manera enunciativa más no limitativa lo siguiente:

- Número de evento.
- Fecha y hora de apertura del evento.
- Fecha y hora de solución del evento.
- Tiempo de solución del evento.
- Numero de Incidente en caso de derivación al proceso de gestión de incidentes.

4.2.1.1.2 Gestión de Requerimientos

Se entenderá como "requerimiento" a cualquier solicitud parte del Instituto hacia **KIO NETWORKS** respecto a los servicios relacionados a la presente Propuesta Técnica. No se considerarán requerimientos los incidentes, problemas, eventos, modificaciones a la CMDB, ni solicitudes de cambio normales y emergentes.

KIO NETWORKS proporcionará un punto único de entrada para todas las solicitudes que no implican un incidente, tales como accesos, permisos, cambios estándares o requerimientos de información, o cualquier requerimiento relacionado a los servicios de la presente Propuesta Técnica, una vez proporcionado y explicado el punto único de entrada, **KIO NETWORKS**, llevará un registro documentado de los requerimientos y/o solicitudes.

Actividades a cargo de **KIO NETWORKS**

- Operar la solución tecnológica para la gestión de requerimientos.
- Proporcionar un medio de comunicación para recibir solicitudes del Instituto a través de los canales que éste último establezca.
- Gestionar la solicitud.
- Asegurar la atención de la solicitud.
- Documentar el cierre de la solicitud.

4.1 Grupo de Gobierno del Contrato y aspectos generales para la prestación de los servicios de la presente Propuesta Técnica

El Instituto informará a **KIO NETWORKS** y a los miembros del Grupo de Gobierno del Contrato (GGC), los cuales definirán, autorizarán y verificarán ante **KIO NETWORKS**, los requerimientos de servicios, así mismo recibirán la información de seguimiento de cada servicio, incluyendo el informe de avances, estado de requerimientos, asuntos, consumos, riesgos, desviaciones, incidentes, eventos, problemas, y cualquier información relacionada al servicio prestado.

KIO NETWORKS ejecutará e informará al GGC del Instituto el seguimiento de cada servicio, informando avances, estado de requerimientos, asuntos, consumos, riesgos, desviaciones, incidentes, eventos, problemas, y cualquier información relacionada al servicio prestado.

KIO NETWORKS gestionará en conjunto con el GGC del Instituto toda la información generada por los servicios descritos en el presente anexo técnico y **KIO NETWORKS** habilitará un repositorio de información donde integrará la información propia del contrato, entre otras, los entregables y documentación probatoria de la prestación de los servicios, a fin de que se cuente con la memoria documental de la operación y gestión de la operación en caso de que entes fiscalizadores soliciten la revisión de la documentación probatoria de la prestación de los servicios, esto no exime la entrega mensual en medios electrónicos y físicos de toda la información que se desprenda de la presente Propuesta Técnica.

KIO NETWORKS se apegará al Marco Tecnológico de Referencia del Instituto en caso de ser necesario, buscando modelos de reutilización, estándares, modelos de referencia públicos relacionados al objeto de la presente Propuesta Técnica.

KIO NETWORKS realizará las actividades técnicas necesarias para gestionar la información operativa relacionada a la ejecución de servicios descritos en el presente anexo técnico, identificando áreas de oportunidad y mejora operativa, mismas que serán informadas al GGC del Instituto para que en su caso sustenten la tomar decisiones en busca de la mejora en la continuidad operativa de los servicios del Instituto. Entregando al GCC la información relacionada a Incidentes, Problemas, Cambios, Eventos y la Base de datos de gestión de configuraciones (**CMDB**).

KIO NETWORKS con el objeto de contribuir al fortalecimiento de la supervisión y vigilancia de la administración del contrato materia del presente servicio y contribuir a las acciones para verificar la procedencia de los pagos, proporcionará al GCC todo el soporte documental acorde a lo establecido en los entregables de la presente Propuesta Técnica, indicando de manera formal las desviaciones respecto a los niveles de servicio acordados, así como la propuesta de cálculo de deductiva o penalización según sea el caso para cada servicio de la presente Propuesta Técnica. Del mismo **KIO NETWORKS** presentará

al GCC la lista de obligaciones (entregables, verbos, entre otros) relacionadas al contrato y estrategia de atención, indicando en cuyo caso, las fechas límites para el cumplimiento de la obligación respetiva.

KIO NETWORKS con base en las solicitudes u órdenes de servicio que genere el Instituto en apego a lo descrito en el presente anexo técnico, presentara al GCC de manera semanal un desglose detallado del trámite que corresponde a la atención de cada una de ella, en cuanto a su procedencia, tiempos límite de respuestas y demás circunstancias que se encuentren establecidas para cada servicio.

KIO NETWORKS proporcionará al GGC con base en la facturación mensual, la proyección del consumo de servicios hacia el final del contrato, que brinde información necesaria al Instituto para la toma de decisiones.

Para lo anterior, **KIO NETWORKS** entregará de manera semanal y mensual, el acumulado de BCF's facturados, con su correspondiente ejercicio presupuestal, proyección y tendencia de gasto durante la vigencia del contrato, así como su clasificación por centro de costo (por Dirección Normativa que consume los servicios) efectuando un prorrateo en caso de infraestructuras transversales.

4.2 Servicio de Continuidad a la Operación y Soporte

4.2.1 Soporte a la Continuidad Operativa

KIO NETWORKS brindará continuidad operativa, gestión, operación y soporte a los Bloques de Construcción Fundamentales, Bloques de Construcción Comunes y los diversos componentes que integren los servicios tecnológicos que soportan las aplicaciones, componentes y servicios digitales del Instituto, a fin de dar cumplimiento a los niveles de servicio en el presente Anexo Técnico.

KIO NETWORKS se apegará a las "buenas prácticas" en los procesos de gestión en materia de TIC, apegadas a la normatividad y los modelos de operación vigentes del Instituto durante la vigencia del contrato, así como incluir al personal y soluciones tecnológicas suficientes para la entrega del servicio.

KIO NETWORKS se sujetará e integrará con los procesos y soluciones tecnológicas que el Instituto establezca en su modelo de operación para la gestión de TI.

KIO NETWORKS establecerá ciclos evolutivos de mejora operativa que aporten al cumplimiento de los niveles de servicio descritos en el presente anexo técnico.

4.2.1.1 Gestión de Servicios

A continuación, se definen los conceptos y las características que de manera enunciativa más no limitativa deben cumplir los procesos que implemente y opere **KIO NETWORKS** durante la vigencia del servicio.

ANEXOS

DIVISIÓN DE CONTRATO

KIO NETWORKS elaborará Programas de Trabajo Detallados que sean necesarios para la puesta a punto de cada uno de los servicios de:

- Servicio de Continuidad y Gestión de la Operación
- Servicio de Operación y Calidad de la Seguridad informática perimetral
- Servicio de integralidad de ambientes distribuidos a nivel nacional y telecomunicaciones
- Servicio de Gestión de Medición del Desempeño de Aplicativos y Componentes Institucionales

3.4.8 Consideración de la Migración de Punto Neutro

El servicio se dará por aceptado cuando se cumplan como mínimo los siguientes criterios:

- Cuando se logre la conexión en capa física y capa de 3 de la nube de **KIO NETWORKS** de servicios ISP al Punto Neutro.
- En el caso del servicio de Internet y redes de MPLS, ejercer la conmutación en ambos "sites", (principal y secundario) para probar la redundancia geográfica.
- En un nodo o inmueble correr el protocolo de pruebas para todos los servicios y aplicaciones que la contratante determine, incluyendo si existe redundancia automática con algún otro proveedor ISP en la última milla.
- Cuando la herramienta de Monitoreo quede instalada en su totalidad para medir los SLA.
- Cuando queden firmados los SLA's
- Cuando corra un mes de tiempo de garantía sobre los servicios.
- Cuando se entregue la memoria técnica de la solución.

En la entrega de documentación para procesos de Incidentes y cambios. Esquema propuesto para la prestación de los servicios solicitados será bajo la modalidad de servicios "Bajo Demanda", la cual se define de forma integral tanto en el anexo técnico como características técnicas de los servicios y en la propuesta económica por un precio unitario. Lo anterior permitirá la modalidad de poder realizar únicamente el pago por servicio devengado. Esta modalidad aplicará para los siguientes servicios:

- Servicios de aprovisionamiento de las soluciones de almacenamiento y recuperación de datos, procesamiento físico, infraestructura de red, y seguridad lógica.
- Servicio de piso blanco y de espacio en rack.
- Servicios de Monitoreo y Control de consumos de infraestructura.

4 CARACTERÍSTICAS DE LOS SERVICIOS PROPUESTOS

El servicio está compuesto por las siguientes categorías:

- Servicio de Continuidad y Gestión de la Operación
- Servicio de Operación y Calidad de la Seguridad informática perimetral
- Servicio de integralidad de ambientes distribuidos a nivel nacional y telecomunicaciones
- Servicio de Gestión de Medición del Desempeño de Aplicativos y Componentes Institucionales

KIO NETWORKS asignará un responsable para dirigir la ejecución y el programa de trabajo de cada servicio, debiendo compartir actividades, recursos y responsabilidades entre los otros servicios de la presente Propuesta Técnica, buscando eficiencias y economías sin comprometer los niveles de servicio.

El objetivo primordial de los servicios de la presente Propuesta Técnica es de garantizar la continuidad operativa, gestión y el soporte de las plataformas, BCFs y BCCs realizando las actividades específicas necesarias para el sano funcionamiento del servicio.

La siguiente imagen muestra de manera esquemática el modelo operativo del servicio objeto de la presente Propuesta Técnica:

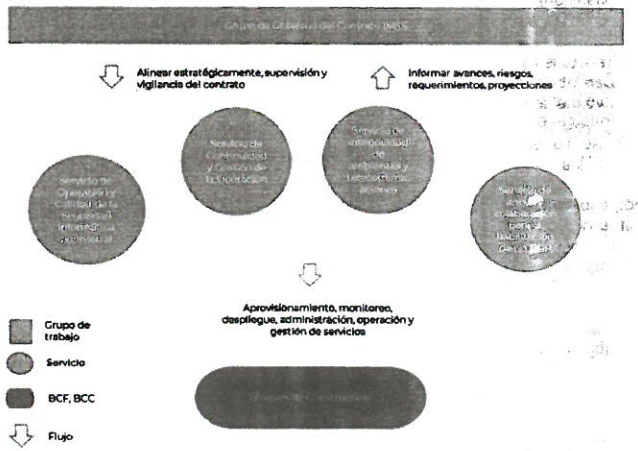


Ilustración 3 Marco Operativo base para el Servicio de Continuidad de la Nube IMSS 2020

Planeación del Arranque	1	Kick-Off y presentación del equipo de trabajo de KIO NETWORKS.	A más tardar 10 días naturales posteriores al Fallo	Plazo ofertado por KIO NETWORKS	N/A
	2	Mesas (sesiones) de trabajo de Planeación del Arranque, entre KIO NETWORKS y el IMSS, convocadas por el Grupo Administrador del Contrato IMSS	Plazo ofertado por KIO NETWORKS	Plazo ofertado por KIO NETWORKS	1
	3	Presentación, por parte de KIO NETWORKS del Plan de Trabajo Detallado	A más tardar 5 días naturales posteriores a la finalización de las Mesas de Trabajo	Plazo ofertado por KIO NETWORKS	2
	4	Análisis y Revisión (en su caso aprobación) del Plan de Trabajo Detallado de parte del Grupo Administrador del Contrato del IMSS	A más tardar 15 días naturales posteriores a la entrega del Plan Detallado de parte de KIO NETWORKS	Plazo ofertado por KIO NETWORKS	3
	5	En caso de aplicar, incluir firma de Acuerdos de Nivel de Operación (OLAs) entre KIO NETWORKS y Terceros Involucrados en los servicios de la presente Propuesta Técnica.	A lo largo de los siguientes 25 días naturales a partir del Kick-Off del proyecto	Plazo ofertado por KIO NETWORKS	1
Actividades de migración de centro de datos actual y	6	Inicio de actividades de migración del centro de datos actual al centro de datos de KIO NETWORKS.	Al día natural siguiente a la aprobación, por parte del IMSS, del	Plazo ofertado por KIO NETWORKS	4

continuidad de la operación de servicios.		incluyendo servicios de punto neutro.	Plan de Trabajo Detallado		
	7	Finalización de actividades de migración del centro de datos actual al centro de datos de KIO NETWORKS incluyendo punto neutro.	Plazo ofertado por KIO NETWORKS	Plazo ofertado por KIO NETWORKS	4
	8	Estabilización de los Niveles de Servicio a la finalización de la etapa de migración.	Plazo ofertado por KIO NETWORKS	Plazo ofertado por KIO NETWORKS	6 y 7
	9	Inicio de los Servicios asociados a la continuidad operativa de los servicios de la presente Propuesta Técnica.	Plazo ofertado por KIO NETWORKS	Plazo ofertado por KIO NETWORKS	N/A
	10	Actividades de Finalización del Contrato.	A más tardar 4 meses naturales antes del día de la Finalización del Contrato	31 de diciembre de 2020	N/A
CIERRE	12	Finalización del Contrato	-	31 de diciembre de 2020	N/A

ANEXO

DIVISIÓN DE CONTRAT

KIO NETWORKS participará en el establecimiento de la hoja de ruta de arquitectura Institucional, así como en el desarrollo la planeación de la implementación para los trabajos de arquitectura conforme a los programas y proyectos establecidos por el Instituto. También integrarse para su operación con los marcos de trabajo vigentes en el Instituto para la gestión de proyectos, modelos de gobierno tecnológicos, modelos de gestión de contratos, etc.

3.4.6.2 Recomendación tecnológica

KIO NETWORKS emitirá recomendaciones y propuestas relacionadas a la continuidad de la operación de los servicios institucionales y de conformidad con el alcance de los servicios de la presente Propuesta Técnica.

3.4.6.3 Evolución tecnológica

KIO NETWORKS presentará como parte del servicio de continuidad de la operación y en caso de que aplique, al Instituto las propuestas de acuerdo a los requerimientos y tendencias tecnológicas que se identifiquen durante la vida del contrato, que fomenten la continuidad de los servicios ofertados en el presente anexo técnico.

3.4.6.4 Gestión del conocimiento

KIO NETWORKS, como parte de los servicios de la presente Propuesta Técnica, consolidará la información y permitir al Instituto acceder a las bases del conocimiento relacionado con los servicios de la presente Propuesta Técnica, vigilando en todo momento el cumplimiento del marco jurídico en conjunto con el Instituto.

3.4.7 Plan de Trabajo General

El Plan de Trabajo General especifica las fases más relevantes del contrato, **KIO NETWORKS** entregará el plan de trabajo y establecerá los tiempos máximos que prevé emplear en cada una de ellas a fin de dar cumplimiento de las obligaciones relacionadas a los servicios de la presente Propuesta Técnica.

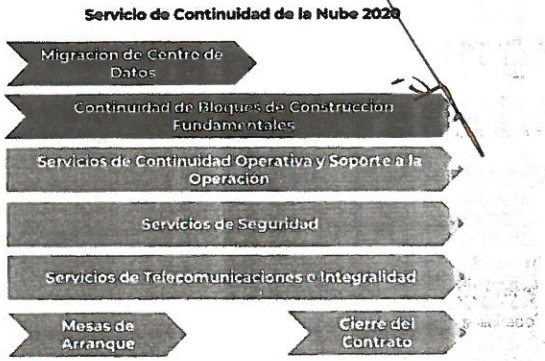


Ilustración 2 Marco de referencia del Plan de Trabajo General

KIO NETWORKS en su propuesta incluye el Plan de Trabajo General, que especifica hitos y fases para el cumplimiento de los servicios de la presente Propuesta Técnica, mismos que serán respetados en todo momento tanto en fechas y compromisos establecidos como en el alcance y funcionalidad ofertada. **KIO NETWORKS** integrará en su propuesta, las definiciones o peticiones de servicio que se establecen en esta Propuesta Técnica y que son vinculadas a una o más fases del Plan de Trabajo General.

A continuación, se especifica de manera enunciativa más no limitativa, una tabla-resumen de los hitos que se prevén en el Plan de Trabajo General para los servicios descritos en el presente anexo técnico, indicando Fase, Identificador del hito en cuestión (ID), el nombre o descripción del hito, las fechas relativas y absolutas de inicio y/o término, cantidad de días naturales máximos de duración por hito que **KIO NETWORKS** oferte.

Tabla 1 Hitos relevantes a considerar en el Plan de trabajo

Fase	ID	Hito	Inicio / Término Máximo del [illegible]	Máxima duración en días naturales*	Precedente(s)
Proceso de Migración de Centro de Datos actual al Servicio de Continuidad de Nube IMSS 2020					

varias de las necesidades del Instituto. Los bloques de construcción son tipificados como: una función o capacidad técnica, un componente de aplicación o un componente tecnológico, por citar algunos ejemplos; los cuales pueden interoperar con otros bloques de construcción, componerse de, o ser parte de, otros bloques de construcción.

Los bloques de construcción representan los elementos categorizados dentro de la taxonomía del Instituto a través del continuo empresarial.

3.4.4.1 Bloques de Construcción Fundamentales (BCF)

Los BCF se definen como aquellos Bloques de Construcción que se encuentran descritos en el Apéndice "Bloques de Construcción Fundamentales".

3.4.4.2 Bloques de Construcción Comunes (BCC)

Los BCC son aquellos Bloques de Construcción que se definen a partir de múltiples BCF, con la finalidad de crear elementos de mayor funcionalidad y complejidad los servicios de la presente Propuesta Técnica, pero con cierto grado de generalidad que hacen factible su reutilización para múltiples soluciones. Los BCC serán definidos de manera conjunta entre **KIO NETWORKS** y el Instituto durante la vigencia del servicio.

3.4.5 Estrategia de disponibilidad y niveles de servicio

Los servicios objeto de la presente Propuesta Técnica consideran los elementos y las acciones necesarias para que dichos servicios se encuentren operando y sean accesibles conforme a los niveles de servicio que requiere el Instituto; para lo cual se alinearán a lo señalado en el MAAGTICSI y las "buenas prácticas" que señala la industria (en particular ITIL), en cada uno de sus componentes y procesos del ciclo de vida de entrega del servicio.

KIO NETWORKS cumplirá con los niveles de servicio establecidos en el presente Anexo Técnico o en el apéndice respectivo, soportado en la capacidad actual de la infraestructura en operación, y en las proyecciones para los nuevos servicios incluidos en el portafolio de servicios del Instituto, incluyendo los siguientes rubros:

- Información relevante que se desprenda en las capacidades de la infraestructura.
- Requerimientos, actuales y previstos, de disponibilidad de los servicios objeto de la presente Propuesta Técnica.
- Disponibilidad de los componentes de la infraestructura de TIC que soportan los servicios del contrato, incluidos los relacionados que sean proporcionados por terceros.
- Riesgos que pudieran materializarse al efectuar adecuaciones a los componentes de la infraestructura que soportan los servicios.
- Costos estimados y validados por el Instituto para llevar a cabo las adecuaciones que permitan obtener la disponibilidad esperada acorde a los niveles de servicio.

- Reporte mensual de la disponibilidad de los servicios para determinar el cumplimiento de los niveles de servicio descritos en el presente anexo técnico, en función de la disponibilidad de la infraestructura y componentes asociados que soportan los servicios.
- Reporte de los incidentes que se han presentado por falta de disponibilidad identificados a través las herramientas de visibilidad del servicio y gestionadas mediante el Servicio de Continuidad Operativa.
- Evaluación de los niveles de disponibilidad de los servicios y de los componentes de la infraestructura que los componentes con respecto a:
- Los niveles de servicio originalmente acordados.
- Los niveles de servicio efectivamente proporcionados.
- Los niveles de servicio que, de acuerdo con el programa de disponibilidad.
- Configuración en una base de datos de gestión de configuraciones (CMDB) y las características de cada componente de la infraestructura que soportan los servicios.
- Mecanismos de comunicación hacia los responsables de los dominios tecnológicos involucrados en los servicios objeto de la presente Propuesta Técnica para que estèn informados de:
- Las oportunidades identificadas para mejorar la disponibilidad de los servicios.
- Recomendaciones sobre los incidentes por falta de disponibilidad.
- Niveles de servicio alcanzados.

3.4.6 Planeación y gobierno

La DIDT ha implementado, como parte de su modelo gobierno, un conjunto de acciones que le permiten enfocar sus iniciativas hacia la habilitación y continuidad de la Estrategia del Instituto, de tal manera que dicha oferta se encuentre alineada con los objetivos y necesidades de negocio del Instituto a nivel estratégico, a través del establecimiento de la demanda de servicios desde un ejercicio de planeación.

Como parte de los procesos de planeación y gobierno de la DIDT establecidos en su modelo de operación, se encuentran estrechamente relacionados los procesos de Planeación Estratégica, pues es a través de estos procesos que se genera el portafolio estratégico de proyectos (PEP) definido por la DIDT.

Los Servicios de la presente Propuesta Técnica, estarán alineados al PEP y de ser necesario, si el Instituto así lo señala, participar en mesas de trabajo para aportar en la definición de dicho instrumento, brindando información respecto de la operación, capacidades y situación actual de los servicios de la presente Propuesta Técnica.

3.4.6.1 Planeación y gobierno

ANEXOS

3.4.2 Características del cómputo en la Nube

Las soluciones de cómputo en la nube disponibles en el mercado en la actualidad admiten diferentes clasificaciones según el aspecto que se tenga en cuenta para realizar dicha clasificación. Con base en las definiciones de industria consideradas en los estándares del Instituto dentro del marco de la Transformación Digital IMSS, se definen tres características fundamentales que marcan la definición de modelos para las soluciones de nube: familias, formas de implementación y capacidades técnicas de **KIO NETWORKS**.

Mediante la combinación de estas tres dimensiones se detallan los distintos modelos de cómputo en la nube existentes en el mercado. Estas tres características, junto con sus diferentes tipos de soluciones asociadas, se pueden representar en un cubo de tres dimensiones. La selección de las características que aplican a los servicios de la presente Propuesta Técnica, se muestra bajo el modelo de cubo en la imagen siguiente:

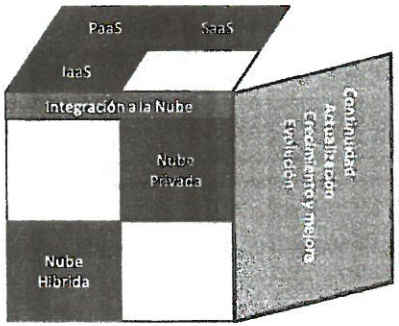


Ilustración 1 Representación gráfica de características y tipos de soluciones de nube seleccionadas

3.4.3 Clasificación por familias de tecnologías como servicio

3.4.3.1 Infraestructura como un servicio (IaaS)

Familia del Cómputo en la Nube consistente en poner a disposición del cliente el uso de la infraestructura informática (capacidad de computación, espacio de disco y bases de datos, entre otros) como un servicio.

Los clientes que optan por este tipo de familia de nube, en vez de adquirir o dotarse directamente de recursos como pueden ser los servidores, el espacio del centro de datos o los equipos de red, optan por

la tercerización o provisión de infraestructura mediante servicios proporcionados por un tercero (externalización en busca de un ahorro en la inversión en sistemas de TI).

Con esta externalización, las facturas asociadas a este tipo de servicios se calculan con base en la cantidad de recursos consumidos por el cliente, basándose así en el modelo de pago por uso.

3.4.3.2 Plataforma como un Servicio (PaaS)

Familia del Cómputo en la Nube, consistente en la entrega como un servicio, de un conjunto de plataformas informáticas orientadas al desarrollo, pruebas, despliegue, alojamiento y mantenimiento de los sistemas operativos y aplicaciones propias del cliente.

Las principales características asociadas a la Plataforma como Servicio, como solución de nube, se exponen a continuación:

1. Facilita el despliegue de las aplicaciones del cliente, sin el costo y la complejidad derivados de la compra y gestión del hardware y de las capas de software asociadas.
2. Ofrece, a través de redes de servicio IP, todos los requisitos necesarios para crear y entregar servicios y aplicaciones web.

3.4.3.3 Software como un Servicio (SaaS)

Familia del Cómputo en la Nube consistente en la entrega de aplicaciones como servicio, siendo un modelo de despliegue de software mediante el cual **KIO NETWORKS** ofrece licencias de su aplicación a los clientes para su uso como un servicio bajo demanda.

Los Proveedores del Software como Servicio pueden tener instalada la aplicación en sus propios servidores Web (permitiendo a los clientes acceder, por ejemplo, mediante un navegador web), o descargar el software en los sistemas del servicio de nube. En este último caso, se produciría la desactivación de la aplicación una vez finalice el servicio o expire el contrato de licencia de uso.

La solución de cómputo en la nube de Software como Servicio puede estar orientada a distintos tipos de clientes según su condición, por ejemplo:

- Servicios de productividad en la nube.
- Correo electrónico.
- Escritorio en la nube.
- Colaboración.

3.4.4 Bloques de construcción

Para fines de la presente Propuesta Técnica un bloque de construcción (BB, Building Block por sus siglas en inglés) se entiende como un componente unitario o aislado del modelo completo de la arquitectura que describe el modelo completo. Representa un paquete de funcionalidad definido para satisfacer una o

menos tres veces en un mismo mes) que se traduzca en una afectación a los niveles de servicio y operación institucional.
- Actualizaciones tecnológicas que correspondan, que deberán traducirse en ajustes, sustituciones, reemplazos, compensaciones, escalamientos, adaptaciones y demás acciones análogas que reflejen la forma en que KIO Networks entrega al Instituto cada uno de los servicios que se comprenden en esta Propuesta Técnica.
- Actividades continúas de mantenimiento tecnológico a fin de mejorar la experiencia de servicio entregado al Instituto, así como mejorar los niveles de servicio y aceptación de los usuarios institucionales.

3.3 Mínimos y Máximos

El esquema de consumo de los servicios de la presente Propuesta Técnica será basado en mínimos y máximos, los cuales serán devengados en una primera etapa por los servicios de migración de centro de datos, por el consumo de BCF conforme a la "Relación de inventario actual de Centro de Datos"; de manera similar se consumirán los servicios de Centro de Operaciones de Seguridad y del Centro de Continuidad Operativa que serán considerado a partir de la toma en administración de los servicios. A partir de dicho momento, se consumirán los BCF y los BCC sobre demanda, tal y como se establece a lo largo del presente documento.

3.4 Arquitectura de referencia de la presente Propuesta Técnica

En el marco de la Transformación Digital IMSS, se establece una estrategia basada en un modelo de 'nube', que busca fomentar la reutilización, recursos compartidos, y agilidad en el despliegue de soluciones y servicios, previendo la capacidad para acceder de manera flexible a un diverso número de recursos informáticos virtuales asignados de forma ágil y dinámica, obteniendo así la capacidad de procesamiento, almacenamiento, respaldos, seguridad y comunicaciones necesarios.

En las siguientes subsecciones se presenta un marco teórico de referencia sobre el concepto de nube; en ningún momento se deberán considerar como requerimientos puntuales si no son señalados explícitamente en alguna otra sección de la presente Propuesta Técnica.

3.4.1 Capacidades del cómputo en la nube

Según los mismos estándares citados anteriormente, para poder describir eficazmente cuáles son las claves del concepto del Cómputo en la Nube, se recurre a una serie de capacidades o características principales que lo diferencian de los sistemas tradicionales de explotación de las TIC. Entre las capacidades asociadas al Cómputo en la Nube se encuentran las siguientes:

1. **Facturación basada en el consumo.** - Una de las características principales de las soluciones de nube es el modelo de facturación basado en el consumo, es decir, el pago varía en función del consumo que se realiza del servicio en la nube contratado, por lo que el pago es sobre servicios debidamente devengados.
2. **Abstracción.** - Característica o capacidad de aislar los recursos informáticos contratados a **KIO NETWORKS** de servicios en la nube de los equipos informáticos del cliente. Esto se consigue gracias a la virtualización, con lo que la organización usuaria no requiere de personal dedicado al mantenimiento de la infraestructura, actualización de sistemas, pruebas y demás tareas asociadas que quedan del lado del servicio contratado, al mismo tiempo, que se mantiene un orden y gobierno para evitar el caos en el consumo de virtualización.
3. **Agilidad en la escalabilidad (elasticidad).** - Capacidad que permite aumentar o disminuir las funcionalidades ofrecidas al cliente, en función de sus necesidades puntuales. Esta característica, relacionada con la de Facturación basada en el consumo, evita los riesgos inherentes de un posible mal dimensionamiento inicial en el consumo o en la necesidad de recursos.
4. **Multi-Consumidor.** - Capacidad que otorga la nube para permitir que varios consumidores (aplicaciones, usuarios, áreas del Instituto o inclusive terceros como Instituciones) compartan los medios y recursos informáticos, permitiendo la optimización de su uso.
5. **Autoservicio bajo demanda.** - Esta capacidad permite al consumidor acceder de manera flexible a las capacidades de computación en la nube de forma automática a medida que las vaya requiriendo, sin necesidad de una interacción humana con su **proveedor** o **proveedores** de servicios en la nube.
6. **Acceso sin restricciones.** - Capacidad consistente en la posibilidad ofrecida a los consumidores de acceder a los servicios consumidos de la nube en cualquier lugar, en cualquier momento y con cualquier dispositivo que disponga de conexión a redes de protocolo TCP/IP o a la red privada del Instituto en el caso de la Nube Privada. El acceso a los servicios de la nube se realiza a través de la red, lo que facilita que distintos dispositivos, tales como teléfonos móviles, dispositivos PDA u ordenadores portátiles, puedan acceder a un mismo servicio ofrecido en la red mediante mecanismos de acceso comunes.

KIO NETWORKS cubrirá a través de los servicios de la presente Propuesta Técnica las capacidades de cómputo en la nube antes mencionadas o las necesarias para su operación.

ANEXO

DIVISIÓN DE CONTRA

Una vez iniciados los servicios, **KIO NETWORKS** brindará continuidad operativa a los servicios de la presente Propuesta Técnica y dar cumplimiento al Plan de Trabajo Detallado ofertado, al amparo y cumplimiento del Plan de Trabajo General descrito en el Anexo Técnico, con el cual en cuyo caso efectuará la migración de elementos dispuestos en el Servicio actual de Centro de Datos. Una vez que los BCF correspondientes a la migración se encuentren activos y operando en el Centro de Datos ofertado a entera satisfacción del Instituto, podrán ser incorporados al esquema de contraprestación de pagos mensuales.

En apego al mismo Plan de Trabajo General, **KIO NETWORKS** presenta en su propuesta un programa de trabajo anual para cada uno de los siguientes servicios:

- Servicio de Continuidad y Gestión de la Operación
- Servicio de Operación y Calidad de la Seguridad informática perimetral
- Servicio de Integralidad de ambientes distribuidos a nivel nacional y telecomunicaciones
- Servicio de Gestión de Medición del Desempeño de Aplicativos y Componentes Institucionales

Una vez ofertados y detallados por **KIO NETWORKS** estos planes de trabajo en su oferta, y en su caso revisados, modificados, detallados y finalmente aceptados por el Instituto en las reuniones de inicio del contrato, **KIO NETWORKS** comenzará a realizar las actividades de habilitación, implementación, puesta punto, operación y administración de cada servicio.

El plan de trabajo general propuesto por **KIO NETWORKS** podrá sufrir modificaciones durante su ejecución de acuerdo a las necesidades operativas del Instituto, por ejemplo, en casos donde resulte inviable migrar aplicativos o servicios por la alta concurrencia, alta demanda o estacionalidad de negocio en un periodo especifico, por lo que habrá que esperar las condiciones operativas necesarias que permitan ejecutar la migración, tal es el caso de los periodos de alta recaudación, emisión, dictaminación, cierres presupuestales, por mencionar algunos.

3.1 VIGENCIA

El **Servicio de Continuidad de la Nube IMSS 2020**, se proporcionará el día natural siguiente al acto del fallo al 31 de diciembre del 2020.

3.2 MODALIDAD DEL SERVICIO

El modelo de servicio en el presente Anexo Técnico toma como base el concepto de "servicios administrados bajo demanda", que involucra un precio unitario por unidad devengada en un periodo determinado, así como pago de servicios relacionados a la operación, seguridad, telecomunicaciones y

migración, que brinden la continuidad de la operación a los servicios institucionales que se encuentran alojados en el centro de datos de **KIO NETWORKS** acorde a los niveles de servicio establecidos. El modelo del servicio incluye las siguientes características o funcionalidad:

KIO NETWORKS incluye en su oferta: habilitar, migrar, implementar, configurar, poner a punto, operar y administrar el servicio de Continuidad Operativa de los sistemas actuales de procesamiento y almacenamiento con la siguiente funcionalidad y características:

- Aprovisionamiento de hardware y software bajo una modalidad de servicios administrados bajo demanda.
- Capacidad de soportar operativamente soluciones de TIC complejas a través de la correcta implementación de Bloques de Construcción Comunes (BCC), basados en niveles de servicio y características de los Bloques de Construcción Fundamentales (BCF). Los bloques de construcción fundamentales son las pieza mínimas indivisibles para efecto de facturación y cobranza del presente servicio, mientras que los bloques de construcción comunes son conjuntos de BCF que se agrupan para la habilitación de una solución de negocio, tales como el Expediente Clínico Electrónico o cualquier otro sistema integral operativo, por lo que estos nuevos bloques (BCC) serán considerados para la cuantificación de la deductiva de la infraestructura en caso de falla de un servicio de negocio con afectación a infraestructuras dependientes o correlacionadas con la misma, las cuales dejan de operar por consecuencia de la falla de una infraestructura diferente, lo que ocasionará que las deductivas aplicables incluyan tanto a los BCF afectados, como a los BCC correlacionados que sufren afectación a causa de terceros.
- Monitoreo de la infraestructura y la visibilidad sobre la situación operativa de la infraestructura y de los diferentes servicios tecnológicos, digitales y de información que el Instituto señale.
- Servicios de Soporte a la Operación apegados a las "buenas prácticas" nacionales e internacionales y en general la normatividad aplicable durante la prestación del servicio.
- Servicios operativos de seguridad de la información a través de un Centro de Operaciones de Seguridad (SOC).
- Identificación de actividades para garantizar la escalabilidad, prever disminución y aumentos en la demanda de recursos tecnológicos en función del análisis periódico de crecimiento y uso de recursos.
- Proponer mejoras a la forma de disposición de los BCF y los BCC para generar eficiencias y mejora en el desempeño.
- Gestión continua de problemas conocidos y análisis de los mismos para identificar causas raíz y propuesta de mejora.

KIO NETWORKS incluye como parte del servicio: habilitar, migrar, implementar, configurar, poner a punto, operar y administrar toda la infraestructura necesaria para efectuar las acciones para el abatimiento del rezago tecnológico en infraestructura, sistemas y tecnologías o actualización tecnológica, por medio de:

- En general, todas las acciones de remediación que **KIO NETWORKS** o el Instituto proponga a fin de restaurar los niveles de servicio en caso de falla continua (intermitencias en la operación al

3 ALCANCE DE LA PROPUESTA TÉCNICA

KIO NETWORKS incluye en su propuesta realizar las actividades necesarias para brindar continuidad operativa a los servicios de la presente Propuesta Técnica, para el aprovisionamiento de infraestructura de procesamiento, almacenamiento, respaldos, comunicaciones, licenciamiento, seguridad informática perimetral y en su caso actividades de migración de centro de datos para que el Instituto opere tal y como se describe en el apéndice "Relación actual de Infraestructura en Centro de Datos y proyección de crecimiento", durante el periodo del 1 de enero al 31 de diciembre de 2020, incluyendo el proceso de migración necesario de centro de datos conforme al Plan General de Trabajo ofertado por **KIO NETWORKS**, tomando las medidas necesarias para garantizar la continuidad del servicio actual.

KIO NETWORKS ofrece en su propuesta económica el costo del concepto de migración bajo el rubro "migración de centros de datos", incluyendo los tiempos de posible afectación a la operación debido a los procesos de migración de información, aplicativos, sistemas y servicios electrónicos o digitales del IMSS del Centro de Datos Actual a la infraestructura ofertada por **KIO NETWORKS**, tanto al interior del Instituto como con los Organismos con los que éste interopera, tales como Servicio de Administración Tributaria (SAT), Registro Nacional de Población (RENAPO), Comisión Nacional Para el Sistema de Ahorro para el Retiro (CONSAR), Infonavit, ProceSar, Afores, Bancos, Instituto Nacional Electoral (INE), entre otros, con los cuales el IMSS intercambia información e interopera procesos de negocio en su gran mayoría en línea o mediante procesos de bloques sincronizados, incluyendo los procesos de sincronización que se realizan diariamente entre los principales sistemas y servicios operados en el centro de datos administrado y el ecosistema IBM Mainframe ubicado en los centros de datos Institucionales, en los que se sincroniza diariamente la información de recaudación, vigencia de derechos, movimientos Afiliatorios y en general toda la sincronización entre los principales sistemas y aplicativos institucionales.

Adicionalmente, **KIO NETWORKS** incluye en su propuesta la habilitación de infraestructura, así como mantener la continuidad operativa de la solución de conectividad en red denominada "Punto Neutro", la cual concentra los enlaces de telecomunicaciones de las diferentes redes de telecomunicaciones del IMSS y proporcionadas por diversos Proveedores de servicio, así como los enlaces de telecomunicaciones de los principales organismos públicos y privados con los que el Instituto interactúa. Esto es, proporcionar la conectividad en red para los aproximadamente 3,000 inmuebles del IMSS donde interoperan con los sistemas y aplicativos ubicados en los Centros de datos centralizados, de igual manera realizan las consultas e interacciones con organismos terceros.

Así mismo, **KIO NETWORKS** incluye en su propuesta la habilitación de infraestructura, así como la continuidad del servicio del centro de datos móvil ubicado en el Centro Médico Nacional de Occidente, en Guadalajara Jalisco, el cual contempla los servicios virtualizados de cada uno de los aproximadamente 3,300 usuarios a través de aproximadamente 1,300 dispositivos clientes ligeros, así como todo el procesamiento y almacenamiento y sistemas de virtualización de cómputo que se requieren para soportar la solución citada.

Finalmente **KIO NETWORKS** incluye en su propuesta que se requiere la habilitación de infraestructura, así como la continuidad del servicio de los aproximadamente 660 servidores de cómputo denominados "autocontenidos" los cuales se encuentran distribuidos a nivel nacional y que permiten la operación local

INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

0402

de los Sistemas Integrales de Medicina Familiar (SIMF), SAI Farmacia, así como sistemas propios de cada Unidad Médica, los cuales interactúan con los sistemas de cómputo centralizados que operan en el Centro de Datos Administrado.

KIO NETWORKS ofrece en su propuesta la habilitación, instalación configuración, puesta a punto, interconexión de infraestructura, así como la migración de cada uno de los sistemas, aplicativos y servicio electrónicos que de forma enunciativa mas no limitativa, se enlistan en el apéndice 3, cuya operación debe garantizar la continuidad de los servicios que el Instituto presta a derechohabientes, patrones, pensionados, trabajadores del Instituto y público en general, a fin de interoperar dentro del ecosistema de infraestructura tecnológica del Centro de Datos administrado así como con los Centros de Datos Institucionales ubicados en Monterrey, Cd. De México y Guadalajara, además de los ecosistemas de infraestructura tecnológica con los que el IMSS interopera tales como: SAT, RENAPO, Procesar, INFONAVIT, Bancos, Instituto Nacional Electoral, Afores, CONSAR, entre otros.

KIO NETWORKS realizará las actividades correspondientes para soportar y operar la infraestructura, aplicaciones y servicios en cualquiera de las modalidades descritas en el presente anexo técnico, garantizando los niveles de servicio señalados en el apartado "Niveles de Servicio" a fin de brindar continuidad a los procesos de negocio internos y externos al IMSS.

El alcance de los servicios descritos en esta Propuesta Técnica comprende los siguientes elementos, conforme a los servicios descritos más adelante:

- Continuidad operativa y aprovisionamiento bajo demanda de los Bloques de Construcción Fundamentales (BCF) conforme se especifica en el Apéndice "Bloques de Construcción Fundamentales" correspondiente, de acuerdo con cada solicitud específica del Instituto.
- Aprovisionamiento bajo demanda de los Bloques de Construcción Comunes (BCC), partiendo de un ejercicio de planeación con el Instituto para determinar las diferentes plataformas que se requieren; y con base en ellas, establecer la definición y habilitación de los BCC a partir de los BCF.
- Monitoreo y vigilancia del funcionamiento y desempeño de los BCF y BCC, así como de los servicios digitales y de información, y los sistemas informáticos y canales digitales que los soportan y se determinen por el Instituto.
- Continuidad Operativa de la interconexión entre múltiples redes privadas de telecomunicaciones a través de un Punto Neutro de intercambio de tráfico, así como el despliegue de canales de acceso con otras nubes tanto públicas como privadas, en la que destaca el acceso a Internet y varias dependencias públicas, mismas que se identifican en el apéndice "Relación actual de la Infraestructura en Centro de Datos".
- Continuidad Operativa y en su caso aprovisionamiento e instalación de cada nodo de extensión de la nube privada, configuración, puesta en marcha, operación, mantenimiento, soporte y administración de Puntos de Acceso a la Nube Privada con capacidad de despliegue del servicio de Escritorio en la nube.
- Provisión de servicios de administración y monitoreo relacionados a los BCF y BCC de la solución.
- Seguridad y autocontenidos

INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

0403

ANEXO

A través de la operación de los servicios tecnológicos en el actual centro de datos tercerizado, el Instituto ha atendido desde agosto de 2013 a junio del 2019, los siguientes trámites:

- 656.4 millones de trámites digitales.
- Recaudación de aproximadamente $1,400 millones de pesos diarios.
- Movimientos Afiliatorios de 986 mil patrones.
- 51 millones de pagos referenciados.
- 11 millones de citas médicas desde la app móvil.
- 9.1 millones de expedientes electrónicos.
- 14.4 millones de recetas electrónicas expedidas.
- 18.5 millones de constancias de semanas cotizadas.
- 128.1 millones de avisos para control de servicios integrales.
- 8.4 millones de cuentas por pagar.
- De 5 a 7 millones de consultas de vigencia de derechos diarias,
- Operación de aproximadamente 160 sistemas, aplicativos y servicios en el centro de datos administrado principalmente de temas de Afiliación, Incorporación, Recaudación, Cobranza, Pensionados, Prestaciones Médicas, Financieros, Administrativos y Jurídicos, entre otros.

Los servicios del centro de datos tercerizado también apoyan temas médicos, dentro de los que destacan los siguientes servicios **diarios.**

- 504 mil 776 consultas.
- 54 mil 958 urgencias.
- 3 mil 861 intervenciones quirúrgicas.
- Mil 36 partos.
- 353 mil 634 consultas de especialidad.

El centro de datos tercerizado también apoya en temas de recaudación, de tal manera que el Instituto recauda aproximadamente 1,400 millones de pesos diarios.

Finalmente, este tipo de servicios reflejan la necesidad de brindar la continuidad en la operación y gestión de la operación 7X24X365 a fin de garantizar los servicios que el Instituto ofrece a los derechohabientes, patrones, contribuyentes, pensionados, personal institucional y público en general.

En el **Apéndice "Relación de Infraestructura actual en Centro de Datos y proyección de crecimiento"** se describe la relación de la infraestructura que abarcan dichos sistemas legados y plataformas, misma que será considerada como la línea base de estimación de costos a partir de la migración y puesta en producción de los servicios de descritos en el presente anexo técnico.

KIO Networks

INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

Para lo anterior, **SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.** en adelante **KIO NETWORKS,** es una empresa fundada en 2002, con capital 100% mexicano ofrecerá el servicio de habilitación de infraestructura tecnológica, migración de dicha infraestructura, servicios digitales y aplicaciones a su centro de datos a fin de garantizar la continuidad operativa de los servicios del Instituto que actualmente se encuentran alojados en el Centro de Datos tercerizado.

KIO Networks

INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

2 OBJETIVO DE LA PROPUESTA TÉCNICA PARA EL SERVICIO

Brindar continuidad operativa de los servicios que permiten al Instituto disponer de las capacidades de procesamiento, almacenamiento, respaldo, comunicaciones, seguridad, plataformas tecnológicas y software bajo las **modalidades de despliegue** siguientes:

- **M1**: Centro de Datos externo (Centro de Datos Primario),
- **M3**: Extensión de Nube Privada (ENP) en los puntos con mayor demanda transaccional de operación de los servicios del Instituto,
- **M5**: Instalaciones designadas por el Instituto, y
- **M6**: Ambientes no productivos para el apoyo a la evolución y desarrollo tecnológico

Estos servicios serán consumidos en tres modalidades:

- Los servicios relacionados a lo que se define como **"Nube Privada"**, soportan entre otros, sistemas transaccionales del Instituto, aplicativos y tecnologías para servicios digitales y de información, bases de datos, medios de almacenamiento, software de productividad, y en general, aquellas tecnologías que están definidas expresamente para utilización del personal o para otorgar al público un servicio del IMSS bajo control del mismo. Estos servicios deberán extenderse en las modalidades de despliegue de: Centro de Datos externo (Primario) y en Nodos de Extensión de la Nube Privada que se desplegarán conforme a lo indicado de manera referencial en el apéndice "Ubicaciones Geográficas".
- Los servicios relacionados a lo que se define como **"Nube Híbrida"**, soportan los servicios aplicativos, digitales y de información, que requieren la interconexión con nubes públicas, privadas y comunitarias. Estos servicios contarán con la capacidad de intercambio de tráfico entre redes de telecomunicaciones, despliegue de canales digitales con reglas específicas de comunicaciones y seguridad, así como la capacidad de extensión de la nube híbrida en regiones geográficas estratégicas para mejorar la experiencia a usuarios externos en la entrega de servicios.
- Los servicios que se definen como de **"Integración a la Nube Privada"**, se refieren a la capacidad de consumo tecnológico en las instalaciones designadas por el Instituto, con la finalidad de lograr algún nivel de integración, desde la capacidad de ser accedida a nivel telecomunicaciones, hasta poder consumir o entregar información desde o hacia la Nube Privada.

Los diferentes servicios incluidos dentro de la presente Propuesta Técnica serán diferenciados tanto por la modalidad de despliegue como la modalidad de Nube. La modalidad de despliegue de Ambientes no productivos aplicará a las tres modalidades de nube: Privada, Híbrida y de Integración a la Nube Privada.

Los servicios serán medidos a través de acuerdos de Niveles de Servicio, para buscar un uso eficiente y eficaz de los servicios y soluciones, apego a procesos determinados por la normatividad del Instituto, así como el suministro de hardware y software para soporte de las aplicaciones del Instituto, lo que permitirá:

- Flexibilizar y agilizar la atención gradual de requerimientos de infraestructura tanto física como virtual.
- Mantener niveles de operación y de seguridad para la Institución.
- Continuidad en la operación de los servicios digitales y de información, así como de los sistemas informáticos del Instituto.
- Contar con alojamiento de las capacidades de infraestructura y almacenamiento.
- Establecer una estrategia en materia tecnológica para el procesamiento y almacenamiento de información del Instituto, así como el de las plataformas que soportan servicios digitales y de información.
- Monitorear el desempeño de los recursos, dar visibilidad de la disponibilidad de servicios digitales y de información, así como la ejecución de actividades de aprovisionamiento y mantenimiento de infraestructura y plataformas con base en Acuerdos de Nivel de Servicio (SLA's).
- Mantener un esquema de atención a derechohabientes, patrones, proveedores, terceros relacionados y/o público en general que ocupe las diversas aplicaciones, servicios digitales y de información que el Instituto ofrece a través de los diversos canales de atención del Instituto, incluyendo portal de Internet (www.imss.gob.mx), conexiones con terceros, ventanilla, notificaciones y canal móvil, así como contribuir a la transformación digital del Instituto y la atención que presta a sus derechohabientes y patrones.

2.1 RESUMEN DEL ENTENDIMIENTO DE LA SITUACIÓN ACTUAL

Durante el periodo del 2016 al 2019, el Instituto ha contado con un centro de datos primario, administrado por un tercero. En ese mismo periodo, el Instituto ha brindado continuidad de los servicios del Instituto y desplegado plataformas tecnológicas para la generación de servicios digitales a través de múltiples canales de atención.

El servicio actual de centro de datos tercerizado ha permitido la operación de diversos sistemas sustantivos del Instituto, dando cobertura a la operación institucional de al menos:

- 84 millones de asegurados y derechohabientes,
- Aproximadamente 1 millón de patrones,
- Aproximadamente 3 millones de pensionados.
- Aproximadamente 460,000 empleados IMSS.
- Aproximadamente 3,000 inmuebles IMSS.

ANEXO
DIVISIÓN DE CON

Índice de Ilustraciones

1 OBJETIVO DEL DOCUMENTO

Elaborar la Propuesta Técnica que satisfaga los requerimientos y las especificaciones técnicas de los bienes y servicios de TIC que requiere el Instituto Mexicano del Seguro Social en materia de los Servicios de Continuidad de la Nube IMSS 2020.

Sixsigma Networks México S.A. de C.V; en adelante **KIO Networks**, acepta la totalidad de las obligaciones de los capítulos y secciones contenidos en la Ficha Técnica y sus Anexos, así como las observaciones y/o comentarios que resulten de la solicitud de aclaraciones y manifiesta la aceptación y compromiso explícito en todas y cada una de las solicitudes efectuadas como parte de los servicios requeridos.

ANEXOS

DIVISIÓN DE CONTRATOS

SOLICITUD DE COTIZACIÓN

"SERVICIO DE CONTINUIDAD DE LA NUBE IMSS 2020"

ID-01a: Aceptación de la totalidad de Capítulos y Secciones del Anexo Técnico

ÍNDICE

CONTENIDO

No.	Nombre del Entregable	Descripción	Periodicidad	Fecha límite de entrega
17	Informe de la implementación de actualizaciones de las versiones del Sistema Operativo, Base de Datos, Middleware, componentes y/o Subsistemas	Documento que contiene evidencia de las actualizaciones de versionamiento del software	Mensual	1 mes
18	Reporte de los certificados que caducan	Informe de caducidad o vigencia de los certificados de seguridad instalados en los ambientes soportados. (por evento, 90 días naturales antes del vencimiento).	Mensual	1 mes
19	Informe Mensual del Servicio (Informe de las versiones de Sistema Operativo).	Documento que continúen las versiones del sistema operativo	Mensual	1 mes
20	Documento con evidencia de la herramienta tecnológica para la visibilidad de los servicios	Un documento que muestre las funcionalidades y alcances de la herramienta	Mensual	1 mes
21	Reporte de Gestión de Configuraciones	Documento con los modelados de la CMDB	Mensual	1 mes
22	Reporte de Incidente (Post-Mortem)	Documento que continúen la cronología o en algunos casos la causa raíz que provoco un incidente relevante (Mayor).	Bajo Demanda	72 horas
23	Servicios cotizados eventualmente	Informe por evento de servicios consumidos del catálogo de Servicios.	Bajo Demanda	1 mes
24	Reporte Dictamen Técnico	Documento que continúen el dictamen técnico al cierre del problema	Bajo Demanda	1 mes
25	Plan de Trabajo del Tuning en todos los ambientes que aplique al mes vencido que se ejecutó	Plan de trabajo que se ejecutó para la afinación de configuración de servicios	Bajo Demanda	1 mes

No.	Nombre del Entregable	Descripción	Periodicidad	Fecha límite de entrega
26	Plan para integrar resultados y avances de la consolidación/migración tecnológica en el mes que se realice	Plan de trabajo ejecutado en una consolidación física	Bajo Demanda	1 mes

ANEXOS

DIVISIÓN DE CONTRATOS

12 CATALOGOS DE SERVICIOS

El Catálogo de Servicios de la presente Propuesta Técnica resume los elementos de servicio que son considerados elementos de pago en el contrato correspondiente, y todos ellos guardan relación con servicios descritos en uno o varios apartados de esta Propuesta Técnica. Los costos de los servicios descritos en esta Propuesta Técnica serán pagados por el IMSS a mes vencido, independientemente de si se refieran a servicios bajo un régimen "Unitario Mensual" o a servicios bajo un esquema "Por Evento" (en cuyo caso será liquidado totalmente).

12.1 SERVICIOS AGREGADOS (RECURRENTES)

#	Tipo de Servicio	Modalidad de Consumo	Descripción
Servicio de Continuidad Operativa y Soporte			
1	Infraestructura y Bloques de Construcción Fundamentales	Unitario Mensual	Servicios para el aprovisionamiento, implementación, operación y soporte de Bloques de Construcción Fundamentales y Comunes.
2	Infraestructura y Bloques de Construcción Comunes	Unitario Mensual	Servicios para el aprovisionamiento, implementación, operación y soporte de plataformas de virtualización o extensión de nube que permitan la integración y el despliegue de determinados BCF según se señalan en el Apéndice "Bloques de Construcción Fundamentales" y los BCC que se definan a partir de los mismos.
3	Punto Neutro	Unitario Mensual	Servicios para innovar la forma de interconexión entre distintos Proveedores de enlaces digital mediante una infraestructura multiplataforma y multicarrier, en donde distintos Proveedores de servicio de conectividad interactúan de manera transparente, otorgando así, el intercambio ágil y oportuno de la información necesaria entre las unidades Médico Administrativas del Instituto.
4	Servicios de Continuidad Operativa y Soporte	Unitario Mensual	Servicios para la gestión, ejecución, mantenimiento, soporte y aseguramiento del aprovisionamiento de los servicios del Instituto dentro de los niveles de servicio acordados.
Servicios de Seguridad			
5	Servicio de Administración y Soporte de Componentes de Seguridad	Unitario Mensual	Servicios para aprovisionar, administrar y soportar componentes de hardware de seguridad para proteger la infraestructura informática y la información contenida en dicha infraestructura.

#	Tipo de Servicio	Modalidad de Consumo	Descripción
6	Centro de Operaciones de Seguridad (SOC).	Unitario Mensual	Servicios para gestionar un Centro de Operaciones de Seguridad (SOC) cuyo objetivo es operar y soportar la infraestructura de seguridad y los servicios asociados para proteger los activos de información contenida en dicha infraestructura.
7	Servicio de Control de Calidad de la Seguridad	Unitario Mensual	Servicios para gestionar y ejecutar controles de calidad de seguridad para dar certeza de las configuraciones o servicios para proteger la información contenida en la infraestructura informática la cual puede ser proporcionada por un tercero.

12.2 SERVICIOS DESAGREGADOS (POR EVENTO)

#	Tipo de Servicio	Modalidad de Consumo	Descripción
1	Unidades de Soporte Extendido	Mediante USEs	Servicios para la ejecución de proyectos o servicios que por su naturaleza tienen una demanda de recursos y esfuerzos variables por lo que su alcance y estimación de recursos son acordados previo a su ejecución.

13 PROCESO DE ENTREGA AL TÉRMINO DEL CONTRATO

Una vez concluida la prestación del servicio, **KIO NETWORKS,** entre otras cosas, realizará el proceso de entrega de todo el equipamiento, software, configuración, desarrollos, CMDB, base de datos de conocimiento, diagramas, bases de conocimiento de configuración de: hipervisores, contenedores, sistemas operativos huésped, software especializado, sistemas, aplicativos, servicios, bases de datos, web services, servidores de aplicación, balanceadores, monitoreo y en general de todas las herramientas y funcionalidades de todo lo que haya sido incorporado como parte del proyecto o en su caso, producto del servicio, incluyendo cualquier componente de hardware/software que integre dicho servicio descrito en el presente documento, así como en la propuesta de **KIO NETWORKS. KIO NETWORKS** se sujetará al procedimiento que el **IMSS** requiera para formalizar este proceso.

14 RELACION DE APENDICES

Apéndice 1 Bloque de Construcción Fundamentales
Apêndice 2 Ubicaciones Geográficas
Apéndice 3 Esfuerzos realizados para la migración de centro de datos actual
Apèndice 4 Relación actual de Infraestructura en Centro de Datos y proyección de crecimiento
Apéndice 5 Especificaciones técnicas de seguridad de la información
Apéndice 6 Objetivos y Métricas de Niveles de Servicio
Apéndice 7 Glosario

ATENTAMENTE

Juan Carlos Martínez Valdés
Representante Legal
SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V

ANEXOS
DIVISIÓN DE CONT

Formato de Cotización de los Servicios Administrados de T.I. - ITSS
Instituto Mexicano del Seguro Social - Dirección de Innovación y Desarrollo Tecnológico (DIDT)
Servicios a cotizar

1	Servidor X86	$11,000.00	$0.00	$9,107.00	$9,001.43	Unitario Mensual					$613,932.54	$0.00	$4,400,629.20	$19,322.91	$5,033,884.65	12	$60,406,615.80
2	Incrementos de Módulos de 1 Procesador con 128 threads X86	$6,050.30	$0.00	$0.00	$5,471.00	Unitario Mensual					$296,909.50	$0.00	$0.00	$10,943.31	$307,852.81	12	$3,694,233.72
3	Incrementos de 128GB de memoria RAM X86	$55,005.23	$55,005.23	$0.00	$50,427.40	Unitario Mensual					$2,574,400.58	$447,721.84	$0.00	$100,854.98	$3,122,977.40	12	$37,475,728.80
4	Módulo de Seguridad en Hardware (HSM)	$0.00	$0.00	$0.00	$45,771.00	Unitario Mensual					$0.00	$0.00	$0.00	$45,771.00	$45,771.00	12	$549,252.00
5	Almacenamiento de Datos Individual	$1,837.44	$0.00	$1,837.44	$0.00	Unitario Mensual					$45,936.00	$0.00	$560,631.04	$0.00	$626,567.04	12	$7,518,804.48
6	Incremento de Almacenamiento de Datos Individual de 100GB	$382.00	$0.00	$382.00	$372.85	Unitario Mensual					$1,583,246.28	$0.00	$237,639.77	$108,155.50	$1,929,041.55	12	$23,148,498.60
7	Respaldo de Datos Individual	$592.75	$0.00	$0.00	$0.00	Unitario Mensual					$48,012.55	$0.00	$0.00	$0.00	$48,012.55	12	$576,150.60
8	Unidad de almacenamiento de media categoría para aplicaciones de bajo desempeño	$0.00	$120,350.38	$0.00	$0.00	Unitario Mensual					$0.00	$240,700.76	$0.00	$0.00	$240,700.76	12	$2,888,409.12
9	Incremento en disco de estado sólido 1TB para almacenamiento bajo desempeño	$10,498.74	$0.00	$0.00	$0.00	Unitario Mensual					$10,498.74	$0.00	$0.00	$0.00	$10,498.74	12	$125,984.88
10	Incremento en disco FC solido 1TB usable para almacenamiento bajo desempeño	$4,277.00	$0.00	$0.00	$0.00	Unitario Mensual					$68,441.60	$0.00	$0.00	$0.00	$68,441.60	12	$821,299.20
11	Unidad de respaldo de plataforma abierta	$421,671.00	$255,770.01	$0.00	$0.00	Unitario Mensual					$1,686,267.91	$255,776.81	$0.00	$0.00	$1,942,064.72	12	$23,304,776.64
12	Incremento de bloques de 30TB usables en arreglo RAID 5 para unidades de plataforma abierta	$23,345.81	$0.00	$0.00	$0.00	Unitario Mensual					$140,074.86	$0.00	$0.00	$0.00	$140,074.86	12	$1,680,898.32
	Unidad de Almacenamiento de Datos de alto rendimiento y red SAN	$444,250.82	$0.00	$0.00	$0.00	Unitario Mensual					$444,250.82	$0.00	$0.00	$0.00	$444,250.82	12	$5,331,009.84
	Incremento en discos de estado sólido 1TB para almacenamiento de alto rendimiento	$12,544.00	$0.00	$0.00	$0.00	Unitario Mensual					$100,352.64	$0.00	$0.00	$0.00	$100,352.64	12	$1,204,231.68
15	Unidad individual de respaldos (Portátil)	$0.00	$0.00	$889.77	$0.00	Unitario Mensual					$0.00	$0.00	$280,277.55	$0.00	$280,277.55	12	$3,363,330.60
16	NetIQ Access Manager (Identity Provider)	$2.63	$2.63	$2.63	$2.63	Unitario Mensual					$0.00	$0.00	$0.00	$0.00	$0.00	12	$0.00
17	Sistema Operativo Red Hat Enterprise Linux	$1,231.53	$0.00	$0.00	$615.77	Unitario Mensual					$25,862.13	$0.00	$0.00	$4,926.12	$30,788.25	12	$369,459.00
18	Sistema Operativo SLES	$1,252.99	$0.00	$0.00	$626.50	Unitario Mensual					$11,276.89	$0.00	$0.00	$1,253.00	$12,529.89	12	$150,358.68
19	Sistema Operativo Oracle Linux Server	$669.14	$0.00	$0.00	$669.14	Unitario Mensual					$0.00	$0.00	$0.00	$0.00	$0.00	12	$0.00
20	Sistema Operativo Windows Server 2008	$675.84	$0.00	$0.00	$0.00	Unitario Mensual					$21,620.40	$0.00	$0.00	$0.00	$21,620.40	12	$259,444.80
21	Sistema Operativo Windows 2012	$675.84	$0.00	$0.00	$0.00	Unitario Mensual					$2,702.55	$0.00	$0.00	$0.00	$2,702.55	12	$32,430.60
22	Servidor Virtual RISC SPARC	$93,323.88	$0.00		$0.00	Unitario Mensual					$653,265.74	$0.00		$0.00	$653,265.74	12	$7,839,188.88
23	Incremento de 1 Procesador Virtual con 128 threads RISC	$3,313.01	$0.00		$0.00	Unitario Mensual					$13,252.04	$0.00		$0.00	$13,252.04	12	$159,024.48
24	Servidor Virtual X86	$2,761.96	$2,618.03		$2,743.48	Unitario Mensual					$1,057,144.80	$78,540.98		356650-98	$1,135,685.78	12	$13,628,229.36
25	Incremento Virtualizado Módulos de 1 Procesador Virtual con 8 threads X86	$417.23	$417.23	$0.00	$417.23	Unitario Mensual					$163,136.93	$8,344.60	$0.00	$2,920.61	$174,402.14	12	$2,092,825.68
26	Incremento Virtualizado 8GB de memoria RAM X86	$1,485.89	$1,485.89	$0.00	$1,485.89	Unitario Mensual					$730,013.22	$17,590.68	$0.00	$24,920.13	$772,524.03	12	$9,270,288.36
27	Puntos de Acceso a la Nube		$216.12			Unitario Mensual						$280,940.19			$280,940.19	12	$3,371,282.28
28	Escritorio en la Nube		$372.85			Unitario Mensual						$352,343.25			$352,343.25	12	$4,228,119.00
29	Plataforma de Virtualizacion multi-tecnologia	$617,518.43	$402,508.45		$0.00	Unitario Mensual					$617,518.43	$402,508.45		$0.00	$1,020,026.88	12	$12,240,322.56
30	Punto Neutro	$676,496.15				Unitario Mensual					$676,496.15				$676,496.15	12	$8,117,953.80
31	Conectividad de Enlaces MPLS 5 Gbps redundante activo - activo	$221,471.51	$221,471.51	$221,471.51	$0.00	Unitario Mensual					$221,471.51	$221,471.51	$221,471.51	$0.00	$664,414.53	12	$7,972,974.36
32	Conectividad de Enlaces Lan2Lan 100 Mbps redundante activo - activo	$0.00	$0.00	$46,283.60	$0.00	Unitario Mensual					$0.00	$0.00	$46,283.60	$0.00	$46,283.60	12	$555,403.20
33	UTM para enlaces de banda ancha hasta 100 Mbps	$0.00	$0.00	$3,935.85	$0.00	Unitario Mensual					$0.00	$0.00	$11,807.55	$0.00	$11,807.55	12	$141,690.60
34	UTM para enlaces de banda ancha hasta 10 Gbps	$0.00	$52,330.20	$0.00	$0.00	Unitario Mensual					$0.00	$104,660.40	$0.00	$0.00	$104,660.40	12	$1,255,924.80
35	Balanceador de carga de capas L4-L7	$147,847.68	$0.00	$0.00	$111,477.31	Unitario Mensual					$295,895.32	$0.00	$0.00	$111,477.31	$407,372.63	12	$4,888,471.56
36	Plataforma Nodo de Extensión de Nube Privada - Tamaño grande		$841,589.53			Unitario Mensual						$841,589.53			$841,589.53	12	$10,099,074.36
37	Piso Blanco (m2)	$21,957.15	$0.00		$0.00	Unitario Mensual					$65,571.44	$0.00		$0.00	$65,571.44	12	$786,857.28
	Espacio en Rack	$21,230.63	$0.00		$0.00	Unitario Mensual					$21,230.63	$0.00		$0.00	$21,230.63	12	$254,767.56
	Oracle Business Intelligence	$73,773.16	$0.00	$0.00	$73,773.16	Unitario Mensual					$0.00	$0.00	$0.00	$0.00	$0.00	12	$0.00
40	Tableau Server	$10,191.24	$0.00	$0.00	$0.00	Unitario Mensual					$441,398.52	$0.00	$0.00	$0.00	$441,398.52	12	$5,296,782.24
41	Tableau Desktop	$3,230.60	$0.00	$3,230.60	$0.00	Unitario Mensual					$25,844.76	$0.00	$48,458.93	$0.00	$74,303.69	12	$891,644.28
42	Oracle ODI	$42,725.77	$0.00	$42,725.77	$0.00	Unitario Mensual					$0.00	$0.00	$0.00	$0.00	$0.00	12	$0.00
43	Bases de Datos Oracle - StandAlone	$1,352.99	$0.00	$0.00	$1,352.99	Unitario Mensual					$0.00	$0.00	$0.00	$0.00	$0.00	12	$0.00
44	Bases de Datos Oracle - RAC	$32,756.42	$0.00	$0.00	$32,756.42	Unitario Mensual					$0.00	$0.00	$0.00	$0.00	$0.00	12	$0.00
45	Microsoft SQL Server	$929.57	$0.00	$0.00	$0.00	Unitario Mensual					$929.57	$0.00	$0.00	$0.00	$929.57	12	$11,154.84
46	Subscripciones a Bases de Datos Open Source	$20,201.31	$0.00	$0.00	$20,201.31	Unitario Mensual					$80,805.24	$0.00	$0.00	$40,402.62	$121,207.86	12	$1,454,494.32
47	Java Development Kit	$151.51	$0.00	$0.00	$0.00	Unitario Mensual					$454.53	$0.00	$0.00	$0.00	$454.53	12	$5,454.36
48	Liferay Enterprise 7/24	$51,850.60	$0.00	$0.00	$0.00	Unitario Mensual					$518,506.00	$0.00	$0.00	$0.00	$518,506.00	12	$6,222,072.00
49	Liferay Enterprise 5/6	$0.00	$0.00	$0.00	$37,438.67	Unitario Mensual					$0.00	$0.00	$0.00	$37,438.67	$37,438.67	12	$449,264.04
50	SOA Suite	$82,416.94	$82,416.94	$82,416.94	$82,416.94	Unitario Mensual					$0.00	$0.00	$0.00	$0.00	$0.00	12	$0.00
51	WebLogic	$712.10	$712.10	$712.10	$712.10	Unitario Mensual					$0.00	$0.00	$0.00	$0.00	$0.00	12	$0.00
52	GlassFish	$7,120.96	$0.00	$0.00	$7,120.96	Unitario Mensual					$35,604.79	$0.00	$0.00	$21,362.88	$56,967.67	12	$683,612.04
53	Apache Tomcat	$0.00	$0.00	$0.00	$252.52	Unitario Mensual					$0.00	$0.00	$0.00	$252.52	$252.52	12	$3,030.24
54	Apache HTTPD	$151.51	$0.00	$0.00	$151.51	Unitario Mensual					$9,393.62	$0.00	$0.00	$5,302.85	$14,696.47	12	$176,357.64
55	Oracle BPM	$81,891.95	$0.00	$0.00	$81,891.95	Unitario Mensual					$0.00	$0.00	$0.00	$0.00	$0.00	12	$0.00
56	Servicio de correo electrónico	$7.28	$0.00	$0.00	$0.00	Unitario Mensual					$575,525.25	$0.00	$0.00	$0.00	$575,525.25	12	$6,906,303.00
57	Firewall	$103,528.37	$0.00	$0.00	$0.00	Unitario Mensual					$621,140.22	$0.00	$0.00	$0.00	$621,140.22	12	$7,453,682.64

VAMOS AL FUTURO

	IPS	$269,964.23	$0.00	$0.00	$0.00	Unitario Mensual					$269,964.23	$0.00	$0.00	$0.00	$269,964.23	12	$3,239,570.76
	Anti-Denegación de Servicios (DDoS)	$237,320.06	$0.00	$0.00	$0.00	Unitario Mensual					$474,640.12	$0.00	$0.00	$0.00	$474,640.12	12	$5,695,681.44
	Redes Privadas Virtuales - VPN	$573.86	$0.00	$0.00	$0.00	Unitario Mensual					$1,147.71	$0.00	$0.00	$0.00	$1,147.71	12	$13,772.52
	Gestión Unificada de Amenazas (UTM)	$32,963.42	$0.00	$0.00	$0.00	Unitario Mensual					$164,817.08	$0.00	$0.00	$0.00	$164,817.08	12	$1,977,804.96
	Filtrado de Contenido Web	$275,141.87	$0.00	$0.00	$0.00	Unitario Mensual					$550,283.73	$0.00	$0.00	$0.00	$550,283.73	12	$6,603,404.76
	Antispam	$249,124.39	$0.00	$0.00	$0.00	Unitario Mensual					$496,248.78	$0.00	$0.00	$0.00	$496,248.78	12	$5,978,985.36
	Antimalware	$269,964.23	$0.00	$0.00	$0.00	Unitario Mensual					$269,964.23	$0.00	$0.00	$0.00	$269,964.23	12	$3,239,570.76
	Firewall Especializado en Servicios Web (WAF)	$249,124.39	$0.00	$0.00	$0.00	Unitario Mensual					$496,248.78	$0.00	$0.00	$0.00	$496,248.78	12	$5,978,985.36
	Nodo de red con UTP	$117.55	$371.65	$0.00		Unitario por servicio					$2,586.05	$225,590.03	$0.00	$0.00	$228,176.08	12	$2,738,112.96
	Nodo de red con Fibra Optica	$0.00	$503.06	$0.00		Unitario por servicio					$0.00	$32,195.52	$0.00		$32,195.52	12	$386,346.24
	Switch de 10G de core	$0.00	$9,864.25	$9,864.25	$0.00	Unitario Mensual					$0.00	$135,299.54	$19,326.51	$0.00	$154,626.05	12	$1,855,536.60
	Switch de 1G de distribución	$0.00	$3,772.16	$0.00	$0.00	Unitario Mensual					$0.00	$264,050.85	$0.00	$0.00	$264,050.85	12	$3,168,610.20
	UTM para enlaces a Red Nacional para Impulso de la Banda Ancha (NIBA) de 100 Mbps	No Aplica	No Aplica	$3,935.85	No Aplica	Unitario por servicio					No Aplica		$3,935.85		$3,935.85	12	$47,230.20
	Enlaces Internet 100 Mbps redundante activo - activo	$91,071.43	$0.00	No Aplica	No Aplica	Unitario Mensual					$364,285.71	$0.00			$364,285.71	12	$4,371,428.52
	Sistema de Almacenamiento de datos en RAID5 de 12TB con capacidad de crecimiento hasta 32TB	$59,819.94	$0.00	No Aplica	No Aplica	Unitario Mensual					$4,411,875.38	$0.00			$4,411,875.38	12	$52,942,504.56
	Solución para el cumplimiento WCAG	$323,248.07	No Aplica	No Aplica	$0.00	Unitario Mensual					$323,248.07			$0.00	$323,248.07	12	$3,878,976.84
																Subtotal A	$391,473,689.16
																I.V.A	$62,635,790.27
																TOTAL A	$454,109,479.43

) del rvicio	Nombre del Servicio	Precio unitario	Unidad de referencia	Unidades de consumo para evaluación		Subtotal B
74	Servicio de Soporte al Gobierno de los Servicios de Nube IMSS	$1,500,000.00	Unitario Mensual	12	meses	$18,000,000.00
75	Servicio de Soporte a la Arquitectura Tecnológica para la Nube IMSS	$750,000.00	Unitario Mensual	12	meses	$9,000,000.00
76	Servicio de Soporte para la Integridad de la Nube IMSS	$2,250,000.00	Unitario Mensual	12	meses	$27,000,000.00
77	Servicio de Soporte para la Calidad de la Seguridad de la Nube IMSS	$750,000.00	Unitario Mensual	12	meses	$9,000,000.00
78	Servicio de Soporte para la Operación de la Seguridad de la Nube IMSS	$1,500,000.00	Unitario Mensual	12	meses	$18,000,000.00
79	Servicio de Soporte de Continuidad Operativa de la Nube IMSS	$2,250,000.00	Unitario Mensual	12	meses	$27,000,000.00
80	Servicio de Soporte y Mantenimiento a Licenciamiento Oracle	$3,652,500.00	Unitario Mensual	12	meses	$43,830,000.00
					Subtotal B	$151,830,000.00
					I.V.A	$24,292,800.00
					TOTAL B	$176,122,800.00

Concepto	Subtotal	IVA	Total
Costo unitario de servicios BCFs (Subtotal A)	$ 391,473,689.16	$ 62,635,790.27	$ 454,109,479.43
Servicios de soporte y recurrentes (Subtotal B)	$ 151,830,000.00	$ 24,292,800.00	$ 176,122,800.00
Total	**$543,303,689.16**	**$86,928,590.27**	**$630,232,279.43**

1 El participante deberá indicar, como parte de su propuesta económica, los **Precios Unitarios** que decida ofertar para cada servicio en cada Modalidad de Despliegue, considerarando las
2 Las **únicas celdas** en las que se espera algún valor de parte del licitante, se han sombreado en **color verde.**
3 Para determinar el alcance de cada uno de los servicios mencionados en la tabla, el licitante deberá considerar su **definición correspondiente en el Anexo Técnico**, incluyendo sus
4 se deberán integrar, en ningún precio unitario, **componentes de costo distintos** a los definidos para dicho servicio en el Anexo Técnico del proyecto
5 resente cotización es unicamente para propositos de determinar al posible proveedor más económico. El licitante deberá considerar que los servicios y sus volumetrías por modalidad de
6 Sección 1 debidamente llenada de acuerdo con estas instrucciones, **deberá ser incorporado por el licitante como parte de su propuesta**, tanto de forma impresa -debidamente

Todos los precios que aparecen en esta sección son sin I.V.A.

Fecha de la cotización: 24 de diciembre de 2019

NOTA: Precios firmes durante la vigencia del contrato, expresados en Moneda Nacional.

Nombre de la Empresa: SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.

Nombre del Representante Legal de la Empresa: JUAN CARLOS MARTINEZ VALDES

Cualquier discrepancia que exista entre el resumen de la propuesta técnica y la economica sera motivo de desechamiento

Adjudicación Directa Nacional
Número AA-050GYR019-E384-2019

En la Ciudad de México, siendo las **13:00 horas del día 31 de diciembre del 2019,** en la sala de juntas de la División de Contratación de Activos y Logística; ubicada en la Calle Durango número 291, Quinto Piso, Colonia Roma Norte, Código Postal 06700, Demarcación Territorial Cuauhtémoc, presente el servidor público cuyo nombre y firma aparecen al final del presente documento, con objeto de llevar a cabo la Adjudicación Directa Nacional número **AA-050GYR019-E384-2019**, para la contratación del **"Servicio de Continuidad de Nube IMSS 2020".** ----------

---

---------- **Adjudicación** ----------

Derivado del Acuerdo número **AC-39/SE-15/2019**, mediante el cual el Comité de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social, en la **Sesión Extraordinaria Número 15/2019,** celebrada el 20 de diciembre de 2019, con fundamento en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 3 fracción IX, 22 fracción II, 26 fracción III, 26 Bis fracción I, 28 fracción I, 40, 41 fracción III y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), así como 71 y 85, de su Reglamento, resuelve dictaminar favorablemente por unanimidad la excepción a la Licitación Pública, mediante el procedimiento de Adjudicación Directa para la contratación del **"Servicio de Continuidad de Nube IMSS 2020".** El monto mínimo adjudicado es por **$252,092,911.77 (Doscientos cincuenta y dos millones noventa y dos mil novecientos once pesos 77/100 M.N.)** y el monto máximo susceptible de ejercer es por **$630,232,279.43 (Seiscientos treinta millones doscientos treinta y dos mil doscientos setenta y nueve pesos 43/100 M.N.)**, ambas cantidades **Sí** incluyen el Impuesto al Valor Agregado (IVA), para ello se cuenta con el Dictamen de Disponibilidad Presupuestal número 000000002003-2020 (Se anexa formato CAAS 01 como parte integrante del presente documento). ----------

---

Atendiendo a lo anterior, de conformidad con el artículo 37, fracción IV de la LAASSP y considerando que de esta forma se aseguran las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes para el instituto se adjudica a la empresa **SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.,** conforme a la propuesta económica del proveedor, la cual se da por reproducida en esta parte como si a la letra se insertara, y la cual fue autorizada por el Comité de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social ----------

---

De la consulta a la información publicada en el Sistema Electrónico de Información Pública Gubernamental, denominado "CompraNet", sobre proveedores y contratistas sancionados, así como con el impedimento para presentar propuestas o celebrar contratos no se encontró al proveedor arriba indicado.----------

---

El servicio deberá prestarse de conformidad con los términos y condiciones y anexo técnico emitidos por el área requirente que rigen la presente contratación y tendrá una vigencia a partir del día natural siguiente al de la adjudicación y hasta el 31 de diciembre de 2020. -----

---

De conformidad con el artículo 37 fracción V de la LAASSP, se notifica al proveedor, que la firma del contrato se realizará a más tardar el día **15 de enero de 2020**, en la División de Contratos, sita en la Calle Durango número 291, décimo piso, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, Ciudad de México, en horario de 9:30 a 14:00 y de 16:00 a 18:00 horas, lo anterior de conformidad a lo establecido en el artículo 46 de la LAASSP. Para tal fin deberá de entregar previamente copia y presentar original para cotejo en la División de Contratos de los siguientes documentos: ----------

---

Persona moral.

a) Acta constitutiva y, en su caso, sus respectivas modificaciones.
b) Poder notarial del representante legal que firmará el contrato.

Persona física:

a) Acta de nacimiento o carta de naturalización.

Ambos:

a) Identificación oficial vigente y con fotografía del representante legal.
b) Cédula de Registro Federal de Contribuyentes.
c) Comprobante de domicilio con vigencia no mayor a 3 meses.
d) En su caso, escrito de estratificación de empresa en términos del artículo 3 de la Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa.
e) Escrito en términos del artículo 50 y 60 de la LAASSP.
f) **Opinión positiva de cumplimiento de obligaciones fiscales emitida por el SAT vigente a la firma del contrato, en términos del artículo 32-D del Código Fiscal de la Federación.**
g) **Opinión positiva de cumplimiento de obligaciones en materia de seguridad social vigente a la firma del contrato emitida por el IMSS, en términos del artículo 32-D del Código Fiscal de la Federación y del Acuerdo ACDO.SA1.HCT.101214/281.P.DIR publicado en el DOF el 27 de febrero de 2015.**
h) **Escrito bajo protesta de decir verdad que no desempeña empleo, cargo o comisión en el servicio público o, en su caso, que a pesar de desempeñarlo, con la formalización del contrato correspondiente no se actualiza un conflicto de interés. (Artículo 49 fracción IX de la Ley General de Responsabilidades Administrativas DOF 18-07-2016). (Anexo 3.6)**
i) **Constancia vigente de situación fiscal emitida por el Instituto del Fondo Nacional de la Vivienda para los Trabajadores (INFONAVIT) en los términos establecidos por las "Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de amortizaciones" publicadas en el Diario Oficial de la Federación (DOF) el 28 de junio del 2017.**

ANEXOS

DIVISIÓN DE CONTRATOS

trabajadores registrados en el Instituto, el particular **deberá de manifestar mediante escrito libre, bajo protesta de decir verdad, que no le es posible obtener la multicitada Opinión, justificando el motivo y anexando el documento (resultado de la solicitud de Opinión que le da el Sistema institucional) en el que conste que no se puede emitir la misma.**

En el caso de aquellos patrones (proveedores o contratistas y sus subcontratados) que tengan más de un Registro Patronal ante el Instituto y alguno o más de uno de estos Registros no se encuentre al corriente en el cumplimiento de las multicitadas obligaciones, **no se podrá considerar que se encuentra al corriente en el cumplimiento de dichas obligaciones, aun cuando el registro patronal que haya utilizado para el contrato que se trate si se encuentre al corriente en sus pagos, por lo que deberá regularizar todos sus Registros a efecto de poder obtener la Opinión positiva.**

En caso de que el participante cuente con trabajadores contratados bajo el régimen de honorarios asimilados a salarios, deberá presentar el(los) contrato(s) con los que acredite el régimen de contratación, así como escrito libre en el que manifieste que no se encuentra obligado a inscribirse ante el IMSS debido a tal situación, por lo que no puede obtener la opinión de cumplimiento de obligaciones en materia de seguridad social.

j) **En su caso, convenio de participación conjunta.** (No aplica)

En caso de que el participante se encuentre inscrito en el Registro Único de Proveedores y Contratistas de CompraNet, deberá remitir únicamente la documentación referida en los incisos: **f), g), h) e i).** ----------
---

De conformidad con el artículo 48 de la LAASSP se informa al proveedor que deberá entregar en la citada División de Contratos, la Garantía de Cumplimiento de Contrato dentro de los diez días naturales posteriores a la firma del mismo. ----------
---

De conformidad con el artículo 37 fracción VI de la LAASSP, este Acto es presidido por el Ingeniero Vicente Callejas Serrano, Titular de la División de Contratación de Activos y Logística, de la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos de la Coordinación de Adquisición de Bienes y Contratación de Servicios, conforme al numeral 7.1.3.2.2.3 del Manual de Organización de la Dirección de Administración y el numeral 5.3.8 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de este Instituto. ----------

No existiendo otro asunto que tratar, se da por terminado este procedimiento a las **13:30 horas** del día de su fecha de inicio, esta acta consta de **5 (cinco) hojas**, adjuntándose como parte integrante de la misma **1 (una) hoja del Formato CAAS 01 y 2 (dos) hojas de la propuesta económica,** por lo que la rubrican al margen y firman al calce para la debida

En caso de que el participante:
a) No se encuentre registrado ante este instituto o;
b) Cuente con Registro Patronal pero se encuentre dado de baja o;
No tenga personal que sea sujeto de aseguramiento obligatorio, de conformidad con lo dispuesto por el artículo 12 de la LSS.

No podrá obtener la citada Opinión, por lo cual dicho participante podrá dar cumplimiento a tal requerimiento presentando lo siguiente:

I. **Documento emitido por este Instituto (resultado de la consulta en el sistema para obtener la Opinión), en el que se haga constar que no se puede emitir la Opinión de cumplimiento, de conformidad con la Regla Quinta del Anexo único del ACDO.SAI.HCT.101214/281.P.DIR;**

II. **Escrito libre, bajo protesta de decir verdad, que no le es posible obtener la multicitada Opinión, justificando el motivo y anexando el documento en el que conste que no se puede emitir la misma y;**

III. **En el caso de que el participante manifieste que presta sus servicios a través de trabajadores subcontratados con un tercero, deberá de presentar en tal caso, junto con la documentación citada en los dos párrafos anteriores , la Opinión de cumplimiento de obligaciones del subcontratante, desde luego, vigente y positiva (lo anterior en términos del artículo 15-A de la LSS).**

En caso de que el participante forme parte de un grupo comercial y uno de los entes que forma parte del grupo se encarga de administrar la plantilla laboral de todas las empresas que lo conforman, será necesario que exhiba el documento que acredite la subcontratación para situarse en el supuesto del párrafo anterior.

En caso de que el participante no cuente con trabajadores debido a que celebró contrato de prestación de servicios con otra empresa que es la que tiene contratados a los trabajadores (outsourcing), deberá presentar dicho contrato, así como escrito libre en el que manifieste que no se encuentra obligado debido a tal situación y opinión positiva vigente de cumplimiento de obligaciones en materia de seguridad social de la empresa subcontratada emitida por el IMSS.

En caso de que el participante no cuente con trabajadores, deberá presentar escrito libre en el que manifieste que no se encuentra obligado a inscribirse ante el IMSS, por lo que no puede obtener la opinión de cumplimiento de obligaciones en materia de seguridad social.

Para los casos de contratos que se formalicen con personas físicas que presten sus servicios por sí mismos y por lo tanto no cuentan con un Registro Patronal ni tengan

constancia de notificación de la misma y efectos legales procedentes, la persona que interviene en todas y cada una de las hojas que integran el acta. ----------

Por el Instituto Mexicano del Seguro Social: ----------

Titular de la División de Contratación de Activos y Logística (Área Contratante)	Ing. Vicente Callejas Serrano
Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional (Área Requirente)	Ing. Eduardo Oropeza Ortiz

---

---------- **Fin del Acta** ----------

SIN TEXTO

	INSTITUTO MEXICANO DEL SEGURO SOCIAL **DIRECCIÓN DE ADMINISTRACIÓN** **UNIDAD DE ADQUISICIONES E INFRAESTRUCTURA** **COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS** **COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS**	**Contrato Número** **P0M0026**

ANEXO 3

"DOCUMENTO DE DESIGNACIÓN DE ADMINISTRADOR DEL CONTRATO"

ANEXOS

DIVISÍON DE CONTRATOS

EL PRESENTE ANEXO CONSTA DE **02** HOJAS INCLUYENDO ESTA CARÁTULA

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

SIN TEXTO

GOBIERNO DE MÉXICO | IMSS

DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO
Coordinación de Sistemas de Infraestructura
Tecnológica Institucional

Oficio N° 09 52 76 61 5300/2019001**049**

Ciudad de México, a 24 de diciembre de 2019

Lic. Leonardo Alvarado Velázquez
Coordinador de Servicios
Administrativos de la DIDT
P r e s e n t e

Con relación al procedimiento de contratación para la prestación del **"Servicio de Continuidad de la Nube IMSS 2020".**

Al respecto y a efecto de atender de manera oportuna las necesidades en materia de Tecnología de la Información y Comunicaciones del Instituto Mexicano del Seguro Social, les informo que el suscrito fungirá como **"Administrador del Contrato"**, con fundamento en lo dispuesto por los artículos 2 fracción V, 74, y 84 del Reglamento Interior del Instituto Mexicano del Seguro Social; numeral 4.17 y 5.3.15 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social, y conforme a lo previsto en el numeral 7.1.2., del Manual de Organización de la Dirección de Innovación y Desarrollo Tecnológico vigente, así como el "*ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias*, publicado en el Diario Oficial de la Federación el 23 de julio de 2018.

Sin otro particular por el momento, hago propicia la ocasión para enviarles un cordial saludo.

Atentamente,

Ing. Eduardo Oropeza Ortíz
Coordinador de Sistemas de Infraestructura
Tecnológica Institucional adscrito a la DIDT

ANEXOS
DIVISÍON DE CONTRATOS

EOO/rvm

SIN TEXTO