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

Contrato Abierto para la prestación del "Servicio de Continuidad de la Nube IMSS 2022", que celebran por una parte, el **INSTITUTO MEXICANO DEL SEGURO SOCIAL**, que en lo sucesivo se denominará **"EL INSTITUTO"**, representado en este acto por la **C. ELVIA ASCENCIO MILLÁN**, en su carácter de Apoderada 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 Apoderada 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.- La C. Elvia Ascencio Millán, en su carácter de Titular de la Coordinación Técnica de Bienes y Servicios, cuenta con las facultades suficientes para suscribir el presente instrumento jurídico en su calidad de Apoderada 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 43,730 de fecha 28 de octubre de 2021, otorgada ante la fe del Licenciado José Luis Franco Varela, Titular de la Notaría Pública Número 150 de la Ciudad de México, e inscrita en el Registro Público de Organismos Descentralizados bajo el folio número 97-7-10112021-174804, de fecha 10 de noviembre de 2021, 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 Servicios 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.

"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 la Nube IMSS 2022", solicitado por la Coordinación de Servicios 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 42062493 de conformidad con el Dictamen de Disponibilidad Presupuestal Previo con número de folio 0000161089-2022, emitido por la Titular de la División de Control y Seguimiento al Presupuesto de Operación en Ámbito Central de fecha 17 de mayo de 2022, documento que se agrega en el **Anexo 1 (uno)** del presente contrato.

I.7.- Con fecha 17 de mayo de 2022, la Coordinación Técnica de Bienes y Servicios, a través de la División de Servicios Integrales, mediante Oficio número 095384611CFE/2022/004453, notificó a **"EL PROVEEDOR"** la adjudicación del procedimiento de Adjudicación Directa Internacional bajo la Cobertura de Tratados número **AA-050GYR988-E20-2022**, con fundamento en lo dispuesto en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos, 3 fracción IX, 25, primer párrafo, 26 fracción III, 40, 41 fracción II y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 71 y 85 de su Reglamento, como se detalla en el **Anexo 2 (dos)**, del presente instrumento jurídico.

I.8.- 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 la solicitud de cotización.

I.9.- 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, actualmente Ciudad de México, inscrita en la Dirección General del 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 Núñez 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 más 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 los registros siguientes:

- Registro Federal de Contribuyentes número: **SNM010323EB5**.
- Registro Patronal ante **"EL INSTITUTO"** y **EL INFONAVIT** número: [redacted]

II.5.- Cuenta 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 2.1.29 y 2.1.37 de la Resolución Miscelánea Fiscal para 2022, publicada el 27 de diciembre de 2021 en el Diario Oficial de la Federación, del cual presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

II.6.- Sus trabajadores se encuentran inscritos en el régimen obligatorio del Seguro Social, y al corriente en el pago de las cuotas obrero patronales a que haya lugar, conforme a lo dispuesto en la Ley del Seguro Social, cuyas constancias correspondientes debidamente emitidas por **"EL INSTITUTO"** exhibe para efectos de la suscripción del presente instrumento jurídico.

II.7.- Cuenta 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, del cual presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

En caso de incumplimiento en sus obligaciones en materia de seguridad social, solicita se apliquen los recursos derivados del presente contrato, contra los adeudos que, en su caso, tuviera a favor de **"EL INSTITUTO"**.

II.8.- Cuenta 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, del cual presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

SE CANCELA INFORMACIÓN CONFIDENCIAL TAL COMO: REGISTRO PATRONAL, POR CONSIDERARSE INHERENTE AL PATRIMONIO DE LA PERSONA MORAL, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN III Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016

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

II.9.- 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.10.- 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"** y cualquier otra entidad fiscalizadora, deberá proporcionar la información relativa al presente contrato que en su momento se requiera, generada desde el procedimiento de adjudicación hasta la conclusión de la vigencia, a efecto de ser sujetos a fiscalización de los recursos de carácter federal.

II.11.- 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.12.- 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 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 la Nube IMSS 2022", 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 oficio de notificación 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 **$139,348,438.46 (CIENTO TREINTA Y NUEVE MILLONES TRESCIENTOS CUARENTA Y OCHO MIL CUATROCIENTOS TREINTA Y OCHO PESOS 46/100 M.N.)**, incluye el Impuesto al Valor Agregado (I.V.A.), y por la cantidad máxima de **$348,371,096.17 (TRESCIENTOS CUARENTA Y OCHO MILLONES TRESCIENTOS SETENTA Y UN MIL**

NOVENTA Y SEIS PESOS 17/100 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 efectuarán pagos a **"EL PROVEEDOR"** una vez proporcionados los servicios, de conformidad con lo dispuesto en los artículos 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 93 de su Reglamento, así como por lo establecido en los Términos y Condiciones que se agregan al presente contrato en el **Anexo 1 (uno)**.

El pago se realizará en pesos mexicanos, en los plazos normados por la Dirección de Finanzas, de acuerdo 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" sin que éstos rebasen los 20 días naturales posteriores a aquel en que **"EL PROVEEDOR"** presente en forma impresa el Comprobante Fiscal Digital por Internet (CFDI), siempre y cuando se cuente con la suficiencia presupuestal, así como con la documentación comprobatoria que acredite la prestación de los servicios, conforme a los numerales cuarto y sexto del capítulo quinto, intitulado, de los Lineamientos para promover la agilización de pago a los proveedores contenidos en el "Acuerdo por el que se emiten diversos lineamientos en materia de adquisiciones, arrendamientos y servicios y de obras públicas y servicios relacionados con las mismas", concordante con los artículos 65 y 66 del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, conforme a lo siguiente:

El contrato y su Dictamen de Disponibilidad Presupuestal (DDP) deberán estar registrados en el Sistema PREI Millenium.

El CFDI deberá presentarse ante la División de Trámite de Erogaciones de la Coordinación de Contabilidad y Trámite de Erogaciones para proceder a su glosa, revisión y, en su caso, aprobación. Dicho CFDI deberá contener el nombre, cargo y firma de autorización del Administrador del Contrato, de quien suscribió la orden de compra o servicio. Asimismo, en dicho CFDI se deberán indicar: número de alta en SAI o número de identificación de pedido-recepción en PREI-Millenium (cuando sea aplicable), número de proveedor, número de contrato, número de garantía de cumplimiento que se haya aceptado, denominación social de la institución que otorga la garantía de cumplimiento y la indicación de que **"EL PROVEEDOR"** cuenta con opiniones positivas y vigentes en materia de aportaciones de seguridad social ante el IMSS e INFONAVIT así como de obligaciones fiscales ante el SAT.

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

En caso de que el devengo por la entrega-recepción no genere número de alta en SAI o número de pedido-recepción en PREI-Millenium, se deberá adjuntar acta de entrega-recepción.

El personal de la División de Trámite de Erogaciones de la Coordinación de Contabilidad y Trámite de Erogaciones no podrá devolver el CFDI presentado por errores que no afecten la validez fiscal del documento o por causas imputables a **"EL INSTITUTO"**.

Para los casos en que no se formalice el presente contrato, la notificación de la adjudicación será el documento con el cual procederá el pago respectivo de los servicios prestados, únicamente para el periodo comprendido entre la notificación de la adjudicación y la fecha en que debió formalizarse el contrato.

Para efectos de lo anterior, la División de Contratos deberá informar al Administrador del Contrato, en un plazo no mayor a 24 horas posteriores al vencimiento del plazo para formalización del instrumento legal, de la falta de formalización del mismo, a efecto de que se realicen las gestiones que correspondan para no recibir los servicios.

"EL PROVEEDOR" deberá expedir sus CFDI en el esquema de facturación electrónica, con las especificaciones normadas en los artículos 29 y 29-A del Código Fiscal de la Federación (CFF), así como las que emita el Servicio de Administración Tributaria (SAT) a nombre de **"EL INSTITUTO"**, con Registro Federal de Contribuyentes IMS421231I45 y en caso de ser necesario como dato adicional, el domicilio en Avenida Paseo de la Reforma Núm. 476 en la Colonia Juárez, C.P. 06600, Demarcación Territorial Cuauhtémoc, Ciudad de México.

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"** archivo en formato XML. La validez de los mismos, será determinada durante la carga y únicamente los comprobantes validos serán procedentes para pago.

El pago se realizará mediante transferencia electrónica de fondos y en la fecha, a través del esquema electrónico interbancario que **"EL INSTITUTO"** tiene en operación, para tal efecto **"EL PROVEEDOR"** deberá proporcionar la documentación requerida por la Coordinación de Tesorería, para dar de alta en el Sistema de **"EL INSTITUTO"**, la cuenta bancaria, (no deberá ser referenciada ni concentradora), CLABE, Banco y Sucursal a menos que éste acredite en forma fehaciente la imposibilidad para ello.

El pago se depositará a **"EL PROVEEDOR"** en la fecha programada, a través del Sistema de Pagos Electrónicos Interbancarios.

El Administrador del Contrato será quien dará la autorización para que la Dirección de Finanzas proceda a su pago de acuerdo a lo normado en el anexo "Normatividad de pago de las 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 de los servicios, 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" podrá optar por cobrar a través de factoraje financiero conforme al Programa de Cadenas Productivas de Nacional Financiera, S.N.C., Institución de Banca de Desarrollo con **"EL INSTITUTO"**.

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 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"**.

"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 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 Reglamento del Código Fiscal de la Federación (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 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.

Al notificar a **"EL PROVEEDOR"** la aplicación de una pena convencional, el Administrador del Contrato deberá solicitar a las áreas de contabilidad la emisión del CFDI de ingreso por dicho concepto y entregarlo a **"EL PROVEEDOR"** para que se compense contra los adeudos que tenga **"EL INSTITUTO"** para con **"EL PROVEEDOR"** o, para que en su defecto, éste proceda a pagar a **"EL INSTITUTO"** la pena convencional.

El pago de los bienes, arrendamientos o servicios quedará condicionado proporcionalmente al pago que **"EL PROVEEDOR"** deba efectuar por conceptos de penas convencionales y/o 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 presente 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.

Las Unidades Responsables del Gasto (URG) deberán registrar los contratos, convenios y su DDP en el Sistema PREI Millenium para el trámite de pago correspondiente.

Los servicios cuya recepción no genere alta a través del SAI o el 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.

Para que **"EL PROVEEDOR"** pueda celebrar un contrato de cesión de derechos de cobro, mismo que 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 autorizar ésta, 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".

En caso de aplicar, en lo referente a los pagos por suscripciones, seguros u otros servicios, que sean de tracto sucesivo, su pago será autorizado previa solicitud del Área Requirente de que se trate.

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 instrumento jurídico, apegándose a las condiciones, alcances y características detalladas en la solicitud de cotización, oficio de notificación de adjudicación del procedimiento del cual deriva el presente contrato, y de acuerdo con lo siguiente:

PLAZO DE LA PRESTACIÓN DEL SERVICIO.- El plazo para la prestación del servicio será a partir del día siguiente de la fecha de adjudicación y hasta el 31 de diciembre de 2022.

La definición de la programación, implementación y desarrollo de los servicios se establece en el Anexo Técnico, que se integra en el **Anexo 1 (uno)** del presente instrumento jurídico.

Asimismo, se deberán observar los plazos establecidos en el Anexo Técnico y los Términos y Condiciones, que se agregan en **el Anexo 1 (uno)** del presente contrato

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 de prestar sus servicios en las ubicaciones señaladas en el Anexo Técnico, Apéndices y 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, Apéndices y en los Términos y Condiciones que se integran en el presente contrato como **Anexo 1 (uno)**, así como a lo ofrecido en la 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 siguiente de la fecha de adjudicación y hasta el 31 de diciembre de 2022.

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 con 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 Federal de Protección a 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.

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

a) DEL SERVICIO.- "EL PROVEEDOR" presentó en su propuesta técnica la documentación necesaria para garantizar el soporte de los fabricantes involucrados en la

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

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 siguientes 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 del artículo 81, fracción VI del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y de la Ley de Instituciones de Seguros y de Fianzas a favor del "Instituto Mexicano del Seguro Social" por un monto equivalente al 10% (diez 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.), 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, 10º 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:

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

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.

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, numeral 14 "Penas convencionales y deductivas", así como en el Anexo Técnico en el Apéndice número 6 "Métricas de Niveles de Servicio", 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"**, por la entrega parcial o deficiente del servicio, se hará acreedor a una sanción conforme los conceptos y porcentajes señalados en los Términos y

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

Condiciones, numeral 14 "Penas convencionales y deductivas", así como en el Anexo Técnico en el Apéndice número 6 "Métricas de Niveles de Servicio", 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.

En caso de que se exceda se podrá proceder a la rescisión del 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

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

cualquiera de las causales que se señalan en el Anexo Técnico, Términos y Condiciones, y las 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 siguientes 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 se compruebe que el servicio ha sido prestado con alcances y características distintas a las pactadas.
4. 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"**.
5. Si la autoridad competente declara el concurso mercantil o cualquier situación análoga o equivalente que afecte el patrimonio de **"EL PROVEEDOR"**.
6. 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.
7. Cuando se sitúe en alguno de los supuestos previstos en el artículo 50 de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público.
8. Si **"EL PROVEEDOR"** no permite a **"EL INSTITUTO"** la administración y verificación a que se refiere la cláusula correspondiente del presente contrato.
9. Cuando incumpla, total o parcialmente, con cualesquiera de las obligaciones establecidas en el presente contrato y sus anexos.

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.

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

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.

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

DÉCIMA OCTAVA.- 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.

DÉCIMA NOVENA.- 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 **"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 la Ley Federal de Transparencia y Acceso a la Información Pública, así como al artículo 8 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

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 información 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.

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.

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

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 Servicios 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, **"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, Apéndices, Propuesta Económica y Oficio de Notificación 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.

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 triplicado, en la Ciudad de México, el **01 de junio de 2022**, quedando un ejemplar en poder de **"EL PROVEEDOR"** y los restantes en poder de **"EL INSTITUTO"**.

POR "EL INSTITUTO" INSTITUTO MEXICANO DEL SEGURO SOCIAL	POR "EL PROVEEDOR" SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.
C. ELVIA ASCENCIO MILLÁN Apoderada Legal	**C. JUAN CARLOS MARTÍNEZ VALDÉS** Representante Legal

ADMINISTRADOR DEL CONTRATO

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

RRSR/HEJ/JMHN/CLGR

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

IMSS	INSTITUTO MEXICANO DEL SEGURO SOCIAL DIRECCIÓN DE ADMINISTRACIÓN UNIDAD DE ADQUISICIONES COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS	Contrato Número S2M0117

ANEXO 1 (UNO)

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

EL PRESENTE ANEXO CONSTA DE **87** HOJAS INCLUYENDO ESTA CARÁTULA

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

INSTITUTO MEXICANO DEL SEGURO SOCIAL

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

FOLIO: 0000161089-2022

[ ] Dictamen de Inversión
[X] Dictamen de Gasto

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

Concepto: OFICIO 654 RECIBIDO EL 16/05/2022 "SERVICIO DE CONTINUIDAD DE LA NUBE IMSS 2022"

Fecha Elaboración: 17/05/2022

Total Comprometido (en pesos): $ 350,000,000.00
Cuenta: 42062493 Serv int Infraestructura Compu
Partida Presupuestaria SHCP: 31904 Servicios integrales de infraestructura de cómputo
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
0.0	0.0	0.0	0.0	77,777.8	38,888.9	38,888.9	38,888.9	38,888.9	38,888.9	38,888.9	38,888.9

DISPONIBLE (en miles de pesos):

0.0	0.0	0.0	0.0	129,143.2	26,430.3	0.0	45,447.3	239,699.1	71,324.1	34,638.0	23,157.0

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 Div de Ctrl y Seguimiento al Pptio de Oper en Ámbito Central

DIA	MES	AÑO

DICTAMINADO DEFINITIVO

DICTAMEN DEFINITIVO

CONTRATO No. _____

IMPORTE DEFINITIVO (EN PESOS) : $ _____ .00

INSTITUTO MEXICANO DEL SEGURO SOCIAL
COORDINACIÓN TÉCNICA DE GESTIÓN PRESUPUESTARIA
DIVISIÓN DE CONTROL Y SEGUIMIENTO AL PRESUPUESTO DE OPERACIÓN EN EL ÁMBITO CENTRAL
CERTIFICACIÓN PRESUPUESTAL

Clave: 6170-009-001

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

Anexo Técnico

SGMP_AnexoTecnico

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

ANEXOS
DIVISIÓN DE CONTRATOS

ANEXO TÉCNICO
Servicio de Continuidad de la Nube IMSS 2022

Contenido

1.	Objetivo del Documento	4
2.	Objetivo	4
3.	Alcance	4
4.	Requerimientos técnicos	5
4.1.	Servicio de Continuidad Operativa y Soporte a la Operación.	7
4.2.	Servicio de Continuidad y Soporte a la Operación de Telecomunicaciones	8
4.3.	Servicio de Continuidad y Soporte de Seguridad	8
4.4.	Migración del Centro de Datos Actual al Centro de Datos Ofertado por el LICITANTE	9
a)	Funcionales	9
b)	No funcionales	10
	Gestión del conocimiento	12
5.	Pruebas	15
6.	Perfil del Proveedor	15
7.	Condiciones técnicas de aceptación de entregables	18
8.	Cronograma de actividades	18
9.	Niveles de servicio acordados que deberán cumplirse	21
9.1.	Definición General de Entrega	22
9.2.	Reportes del Servicio	23
9.3.	Objetivos y Métricas específicas de Niveles de Servicio	25
10.	Requerimientos de arquitectura tecnológica	25
11.	Restricciones e interfaces con otros elementos	26
12.	Firmas de elaboración, revisión y aprobación	27

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	07/12/2021	Elaboración del documento	Héctor Javier Reyes Oropeza
0.2	07/12/2021	Revisión del documento	Javier Cortés López
0.3	07/03/2022	Actualización del documento	Héctor Javier Reyes Oropeza
0.4	18/04/2022	Actualización del documento	Héctor Javier Reyes Oropeza
0.5	06/05/2022	Actualización del documento	Héctor Javier Reyes Oropeza
1.0	06/05/2022	Aprobación del documento	Eduardo Oropeza Ortiz

ANEXOS
DIVISIÓN DE CONTRATOS

1. Objetivo del Documento

Elaborar el documento que contenga los requerimientos y las especificaciones técnicas y de calidad, así como el alcance de la adquisición, arrendamiento o servicio de TIC y SI que se pretenda contratar.

Clasificador Único de las Contrataciones Públicas (CUCOP): 31900004 Servicios a centros de datos (hospedaje, electricidad, video vigilancia, monitoreo, aire acondicionado, servidores y otros)

2. Objetivo

Contratar el **"Servicio de Continuidad de la Nube IMSS 2022"** con el fin de mantener los niveles de servicio proporcionados por el centro de datos actual que brinda la continuidad operativa de los sistemas de alcance nacional del Instituto Mexicano del Seguro Social.

3. Alcance

El **LICITANTE** deberá brindar continuidad operativa, soporte, gestión de la operación de los servicios, aplicaciones y componentes que permiten al Instituto disponer de las capacidades de infraestructura de procesamiento, almacenamiento, respaldo, comunicaciones, seguridad, plataformas tecnológicas y software en infraestructura que será consumida bajo demanda de acuerdo con las necesidades del Instituto y la cual, no deberá contar con anuncio de fin de venta o de soporte durante la vigencia del contrato, que hoy en día se encuentran desplegadas en las siguientes ubicaciones:

- CDP - Centro de Datos Primario (Ambientes Productivos y no Productivos)
- ENP - Extensión de Nube Privada (ATOM)
- SDI - Servicios desplegados en Instalaciones designadas por el Instituto

Centro de Datos Primario

El Instituto habilitará los mecanismos idóneos para garantizar la continuidad operativa, soporte y gestión de la operación de la infraestructura actual del centro de datos primario (aplicaciones, servicios, infraestructura de procesamiento, almacenamiento y respaldo, infraestructura de seguridad y telecomunicaciones), en tanto se lleva a cabo la migración del Centro de Datos Actual a la infraestructura del Centro de Datos ofertado por el **LICITANTE** adjudicado, garantizando la operación de los aplicativos, servicios e infraestructura, de acuerdo a los niveles de servicio establecidos 99.982% de disponibilidad.

Extensión de Nube Privada (ATOM)

El **LICITANTE** adjudicado una vez concluida la migración debe brindar continuidad del servicio, soporte y gestión de la operación 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.

Servicios desplegados en instalaciones designadas por el Instituto

El **LICITANTE** adjudicado una vez concluida la migración debe brindar continuidad del servicio, soporte y gestión de la operación de infraestructura, por ejemplo, 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.

Ambientes no productivos en el Centro de Datos

El **LICITANTE** adjudicado una vez concluida la migración debe brindar continuidad operativa, soporte y gestión de la operación de la infraestructura actual del centro de datos que contenga ambientes no productivos (aplicaciones no productivas, servicios, infraestructura de procesamiento, almacenamiento y respaldo, infraestructura de seguridad y telecomunicaciones), así como su migración del Centro de Datos Actual a la infraestructura del Centro de Datos ofertado por el **LICITANTE**, garantizando la operación de los aplicativos, servicios e infraestructura, de acuerdo a los niveles de servicio establecidos 99.982% de disponibilidad.

Comunicaciones

El **LICITANTE** adjudicado una vez concluida la migración debe brindar continuidad operativa, soporte y gestión de la operación de la solución de telecomunicaciones, incluyendo acciones para habilitación de infraestructura de conectividad en red con la funcionalidad de "Punto Neutro" durante el primer semestre del servicio, la cual deberá tener la capacidad de concentrar los enlaces de telecomunicaciones de las diferentes redes de telecomunicaciones del IMSS y proporcionadas por diversos prestadores de servicio, así como los enlaces de telecomunicaciones de los principales organismos públicos y privados con los que el Instituto interactúa. El servicio debe incluir la conectividad actual de 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.

El **LICITANTE** adjudicado una vez concluida la migración debe brindar la continuidad a los servicios, aplicativos, servicios digitales y de información, así como su interconexión con los centros de datos propios del Instituto o del Gobierno Federal y entidades externas (tales como: SAT, RENAPO, Procesar, Banco de México, INFONAVIT, Bancos, Instituto Nacional Electoral, Afores, CONSAR, entre otros) que permitan el intercambio de información, conforme a los estándares de telecomunicaciones y seguridad definidos por el Instituto.

4. Requerimientos técnicos

El **LICITANTE** adjudicado una vez concluida la migración debe brindar continuidad operativa, soporte y gestión de la operación de la solución de infraestructura de procesamiento, almacenamiento, respaldos, telecomunicaciones y seguridad, así como a las aplicaciones, componentes y servicios digitales del Instituto en sus diversos esquemas desplegados, tales como: Centro de Datos Actual, Nodo de Extensión de Nube y Ubicaciones designadas por el Instituto, así como las que el Instituto designe durante la vigencia del Servicio.

ANEXOS
DIVISIÓN DE CONTRATOS

ANEXO TÉCNICO
Servicio de Continuidad de la Nube IMSS 2022

Los servicios requeridos por el Instituto y que el **LICITANTE** deberá proveer durante la vigencia del servicio son los siguientes:

- Servicio de Continuidad Operativa y Soporte
- Servicio de Continuidad y Soporte de Telecomunicaciones
- Servicio de Continuidad y Soporte de Seguridad

Para cada servicio antes mencionado, se requiere que el **LICITANTE** integre como parte de la ejecución del servicio, los esquemas de Gestión de la Operación y Soporte, así como el Aprovisionamiento de infraestructura bajo demanda relativa a procesamiento, almacenamiento, respaldos, telecomunicaciones y seguridad.

La siguiente tabla muestra de manera enunciativa más no limitativa el esquema de organización de cada servicio:

Nombre del Servicio	Continuidad y Soporte bajo demanda	Aprovisionamiento de Infraestructura bajo demanda
Servicio de Continuidad Operativa y Soporte a la Operación	Servicios bajo demanda de continuidad operativa, gestión de la operación y soporte de la infraestructura de procesamiento, almacenamiento y respaldos, así como a las aplicaciones, componentes y servicios digitales del Instituto en cualquiera de sus capas (web, aplicativa, base de datos, balanceo etc.)	Aprovisionamiento de infraestructura de procesamiento, almacenamiento y respaldos, bajo demanda.
Servicio de Continuidad y Soporte de Telecomunicaciones	Servicios bajo demanda de continuidad operativa, gestión de la operación y soporte referente a componentes e infraestructura de telecomunicaciones, así como la interconexión entre los diferentes ecosistemas Institucionales, así como con otras entidades públicas y privadas.	Aprovisionamiento de infraestructura de telecomunicaciones, bajo demanda.
Servicio de Continuidad y Soporte de Seguridad	Servicios bajo demanda de continuidad operativa, gestión de la operación y soporte referente a componentes e infraestructura de seguridad física y lógica.	Aprovisionamiento de infraestructura de seguridad, bajo demanda.

El **LICITANTE** debe proveer el soporte técnico en caso de falla en un esquema de 7 días 24 horas durante la vigencia del servicio.

A continuación, se describe el objetivo de cada servicio requerido por el Instituto y que el **LICITANTE** adjudicado deberá brindar como parte de los servicios.

Para efectos del anexo técnico y sus apéndices se entenderá como Bloque de Construcción Fundamental (BCF) a cualquier componente mínimo tecnológico de Infraestructura.

4.1. Servicio de Continuidad Operativa y Soporte a la Operación.

El LICITANTE adjudicado una vez concluida la migración debe brindar continuidad operativa, gestión de la operación, habilitación de infraestructura, afinación, puesta a punto, configuración y soporte a los componentes de infraestructura de procesamiento, almacenamiento y respaldos, así como 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.

En el **Apéndice "Relación de Infraestructura Actual en Centro de Datos"** se encuentra la relación de los componentes e infraestructura de procesamiento, almacenamiento y respaldos, así como de telecomunicaciones y seguridad en el actual centro de datos, mismos que el **LICITANTE** debe incluir para brindar continuidad operativa, soporte y servicio a los sistemas, aplicaciones, plataformas e infraestructura de procesamiento, almacenamiento y respaldos.

El **LICITANTE** adjudicado deberá proporcionar el soporte en sitio para los Puntos de Acceso a la Nube cuando el Instituto lo requiera para lo cual, el **LICITANTE** mantendrá el modelo de operación actual para los 4 hospitales que forman parte del Centro Médico Nacional de Occidente en Guadalajara, Jalisco. Cada ENP deberá soportar cuanto menos 400 Puntos de Acceso a la Nube (PAN) y 1,200 Escritorios en la Nube (EN), previendo un crecimiento una capacidad máxima de hasta 1000 PANs y 2000 ENs.

En el **Apéndice "Descripción Detallada de los Servicios de Continuidad de Nube IMSS"** se encuentra el detalle de los componentes:

- **Soporte a la Continuidad Operativa**
  - Gestión de eventos, requerimientos, incidentes, problemas, cambios, configuraciones y liberaciones.
  - Mesa de Servicio
- **Soporte y Gestión de la Operación**
  - Administración de Sistemas Operativos
  - Administración de Bases de Datos
  - Administración de Middleware
- **Soluciones Tecnológicas**
  - Monitoreo
  - Soporte de fabricante
  - CMDB

Durante la vigencia del servicio, el Instituto podrá solicitar procesos de migración de aplicaciones, servicios, e infraestructura, desde el Centro de Datos del **LICITANTE** adjudicado, hacia los Centros de Datos propios del Instituto o del Gobierno Federal, en un esquema de continuidad operativa o de recuperación ante una contingencia o desastre, por lo cual el **LICITANTE** deberá participar en la definición de necesidades tecnológicas y proveer de personal especializado para su ejecución y para mantener la continuidad operativa durante el proceso de migración mencionado, proporcionando todas las facilidades necesarias, tales como: configuraciones, accesos supervisados (sistemas operativos, middleware, bases de datos, virtualizadores, entre otros), arquitecturas o lo que el Instituto determine sea requerido respetando las normas de seguridad y de operación del Centro de Datos origen.

ANEXOS
DIVISIÓN DE CONTRATOS

Para lo anterior el **LICITANTE** adjudicado deberá proporcionar todas las facilidades necesarias para llevar a cabo dicha migración previo análisis de riesgos en el marco de lo establecido en las normas ISO 27001, incluyendo de manera enunciativa más no limitativa lo siguiente:

- Proporcionar acceso supervisado (si es necesario con usuarios administradores) a los equipos e infraestructura de procesamiento, almacenamiento, respaldo, infraestructura de telecomunicaciones y seguridad.
- Proporcionar archivos, configuraciones, ejecución de comandos, extracción de información de la infraestructura de procesamiento, almacenamiento y respaldo, infraestructura de telecomunicaciones y seguridad.
- Proporcionar respaldos, exportaciones, imágenes o elementos similares de los aplicativos o servicios, máquinas virtuales o elementos de infraestructura que permitan el análisis, para instalación, configuración, puesta a punto, o en su caso importación/exportación en Centro de Datos alterno que el Instituto designe para tal fin.
- Permitir la Instalación de agentes en los equipos que se encuentren en el Centro de Datos del **LICITANTE** adjudicado para la extracción, monitoreo, exportación o cualquier componente tecnológico o configuración que el Instituto requiera.
- Proporcionar acceso a los ambientes tecnológicos origen, a fin de realizar la exportación, copiado, clonación o el procedimiento de migración que el Instituto determine.

4.2. Servicio de Continuidad y Soporte a la Operación de Telecomunicaciones

El **LICITANTE** adjudicado una vez concluida la migración debe brindar continuidad operativa, gestión de la operación, habilitación de infraestructura, afinación, puesta a punto, configuración y soporte a los componentes de infraestructura de Telecomunicaciones.

El **LICITANTE** adjudicado proporcionará todos los elementos necesarios como herramientas, personal, hardware y software para la gestión de los servicios que se entregan en los nodos de Extensión de Nube Privada (ENP) y 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.

En el **Apéndice "Descripción Detallada de los Servicios de Continuidad de Nube IMSS"** se encuentra el detalle de los componentes para el Servicio de Continuidad y Soporte a la Operación de Telecomunicaciones:

- Servicio de Soporte de Extensión de Nube Privada
- Punto Neutro
- Servicios de Conectividad y Comunicaciones

4.3. Servicio de Continuidad y Soporte de Seguridad

El **LICITANTE** adjudicado una vez concluida la migración debe brindar continuidad operativa, gestión de la operación, habilitación de infraestructura, afinación, puesta a punto, configuración y soporte a los componentes de infraestructura de Seguridad.

El **LICITANTE** brindará el servicio de Centro de Operaciones de la Seguridad (SOC), que se encuentre físicamente en las instalaciones del **LICITANTE**. El **LICITANTE** brindará la gestión de la seguridad y será responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad, ejecución actividades de revisiones de

seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, así como el establecimiento de acciones de mejora continua.

En el **Apéndice "Descripción Detallada de los Servicios de Continuidad de Nube IMSS"** se encuentra el detalle de los componentes para el Servicio de Continuidad y Soporte de Seguridad:

- Centro de Operaciones de la Seguridad (SOC)
- Administración y Soporte de Componentes de Seguridad

A continuación, se describen los servicios adicionales para el "Servicio de Continuidad de la Nube IMSS 2022", mismos que el LICITANTE deberá incluir como:

4.4. Migración del Centro de Datos Actual al Centro de Datos Ofertado por el LICITANTE

El **LICITANTE** deberá ofertar el servicio de Migración desde el Centro de Datos actual hacia el Centro de Datos ofertado, el cual deberá incluir el proceso de migración de aplicaciones, servicios, infraestructura de procesamiento, almacenamiento, respaldo, seguridad y telecomunicaciones, incluyendo procedimientos, esquemas, tecnologías, herramientas y perfil del personal para ejecutar la migración, que de manera enunciativa más no limitativa deberá integrar las siguientes opciones:

- Migración de aplicación o servicios incluyendo instalación, configuración, puesta a punto de componentes, aplicaciones, bases de datos, middleware o lo necesario para efectuar el servicio de migración.
- Exportación/Importación de máquinas virtuales a través de formatos estándares a la plataforma ofertada por el LICITANTE que permitan poder importar, configurar, poner a punto y validar las diferentes máquinas migradas al centro de datos ofertado.
- Migración de virtualizador a virtualizador con software que permita el movimiento de máquinas entre los virtualizadores actuales y ofertados, incluyendo el software o la plataforma que permita el movimiento, copia, importación, despliegue de máquinas virtuales.
- Migración de infraestructura de almacenamiento y respaldos, usando esquemas de replicación de información o mecanismos que permitan replicar la información en el centro de datos ofertado.
- En su caso, el LICITANTE podrá proponer herramientas o mecanismos adicionales para la migración la cuales deberán ser evaluados y aprobados por el Instituto.

En el **Apéndice "Descripción Detallada de los Servicios de Continuidad de Nube IMSS"** se encuentra el detalle de los componentes para la Migración del Centro de Datos Actual al Centro de Datos Ofertado por el **LICITANTE**:

- Migración de Infraestructura de procesamiento, almacenamiento, respaldo, telecomunicaciones y seguridad.
- Migración de aplicativos, componentes y servicios del Instituto al Centro de Datos Ofertado por el **LICITANTE**.

A continuación, se describen los principales **requerimientos funcionales y no funcionales** que el **LICITANTE** deberá cumplir para la entrega de los servicios objeto del presente anexo técnico, términos y condiciones, así como los apéndices correspondientes:

ANEXOS
DIVISIÓN DE CONTRATOS

a) **Funcionales**

Modelos de Entrega o Despliegue del Servicio

El **LICITANTE** adjudicado deberá desplegar los servicios descritos en el presente anexo en las siguientes modalidades de entrega o despliegue del servicio.

Servicio	Modalidad de entrega o despliegue del servicio
Servicio de Continuidad Operativa y Soporte a la Operación	• Centro de Datos Primario • Ambientes productivos y No productivos • Servicios desplegados en Instalaciones designadas por el Instituto • Extensión de Nube Privada (ATOM)
Servicio de Continuidad y Soporte de Telecomunicaciones	• Centro de Datos Primario
Servicio de Continuidad y Soporte de Seguridad	• Centro de Datos Primario • Servicios de seguridad a nivel nacional

b) **No funcionales**

Disponibilidad y niveles de servicio

El **LICITANTE** deberá proporcionar los servicios objeto del presente anexo técnico y apéndices respectivos, en un esquema de disponibilidad del **99.982%** durante la vigencia del contrato y efectuar las acciones necesarias para que se encuentren operando y sean accesibles para el Instituto alineándose a la normatividad en la materia durante la vigencia del servicio y buenas prácticas que señala la industria, en cada uno de sus componentes y procesos del ciclo de vida de entrega del servicio.

El **LICITANTE** deberá efectuar acciones, vigilancia de los servicios y entregar mensualmente propuestas de mejora acorde a los siguientes rubros que de manera enunciativa más no limitativa se describen:

- Vigilar la disponibilidad de los componentes de la infraestructura de TIC que soportan los servicios del presente anexo técnico, incluidos de ser posible los relacionados que sean proporcionados por terceros.
- Informar de riesgos que pudieran materializarse al efectuar adecuaciones a los componentes de la infraestructura que soportan los servicios.
- Reporte de 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 monitoreo del servicio y gestionadas por cualquiera de los servicios:

- Servicio de Continuidad Operativa y Soporte a la Operación
- Servicio de Continuidad y Soporte de Telecomunicaciones
- Servicio de Continuidad y Soporte de Seguridad

- Cumplimiento de los niveles de disponibilidad de los servicios y de los componentes de la infraestructura con respecto a:

  - Los niveles de servicio originalmente acordados.
  - Los niveles de servicio efectivamente proporcionados.

- Configuración en una base de datos de gestión de configuraciones (CMDB) y las características de cada componente de la infraestructura que soportan los servicios que permita correlacionar incidentes y su impacto.
- Niveles de servicio alcanzados.
- Requerimientos, actuales y previstos, de disponibilidad de los servicios objeto del presente Anexo Técnico.

Gestión de la Base de Datos de Configuraciones

El **LICITANTE** deberá habilitar, configurar, poner a punto, actualizar, brindar continuidad y dar soporte la base de datos de configuraciones (CMDB) e integrar la información de los elementos de configuración (CI) de la infraestructura objeto del presente anexo técnico.

El **LICITANTE** deberá presentar un plan de trabajo para mantener actualizada la información de los elementos de configuración (CI) de manera periódica. El plan de trabajo de la CMDB deberá ser revisado y aprobado por el Instituto en las mesas de trabajo semanales.

La solución de la CMDB que habilite el **LICITANTE** deberá proveer mecanismos que permitan la consulta de información al personal designado por el Instituto. Los mecanismos de consulta podrán ser de manera enunciativa mas no limitativa los siguientes:

- API (Application Programming Interface)
- Pá gina web de consulta de información.
- Exportación de los elementos de configuración y su relación.

Durante la vigencia del contrato de manera mensual y al término del contrato, el **LICITANTE** deberá entregar toda la información de la CMDB al Instituto en un medio electrónico que permita su exportación/importación.

La CMDB habilitada por el **LICITANTE** será utilizada por el Instituto para correlacionar eventos e incidentes y determinar la infraestructura susceptible de impacto colateral, esto es, en caso de un incidente y que por causa de la falla de un componente se vean afectados otros activos tecnológicos, en virtud de que no puedan ser accesados o utilizados hasta el incidente inicial sea corregido. En esos casos, se aplicarán deductivas al componente afectado y a toda la infraestructura susceptible de impacto colateral.

El **LICITANTE** deberá designar un **coordinador de configuraciones**, quien deberá tener las siguientes actividades enunciativas más no limitativas: administración, configuración, actualización de la CMDB, así como notificación al Instituto los cambios realizados.

ANEXOS
DIVISIÓN DE CONTRATOS

El **LICITANTE** deberá entregar y explicar al Instituto de manera mensual un reporte de gestión de configuraciones que soporte las acciones referentes a este apartado, es decir, los cambios efectuados en el mes, incluyendo la infraestructura susceptible de impacto colateral.

Gestión del conocimiento

El **LICITANTE** deberá consolidar, entregar y explicar mensualmente la información relacionada al servicio y permitir al Instituto acceder a las bases del conocimiento y repositorios, mismos que deberán contener de manera enunciativa más no limitativa al menos lo siguiente:

- Memorias técnicas de instalación, distribución, configuración, partición y asignación de la infraestructura física y virtual.
- Manejo y operación de las herramientas de monitoreo, destacando los cambios efectuados desde la última reunión.
- Memorias técnicas de instalación, distribución, configuración y puesta a punto del Sistema Operativo, Bases de Datos, Software propietario y Open Source, capa aplicativa y todos aquellos componentes instalados para la operación de los aplicativos o servicios del instituto.
- Memorias Técnicas de la instalación, distribución, configuración y puesta a punto de los componentes habilitados para proporcionar la conectividad de la red para los aproximadamente 3,000 inmuebles del IMSS donde interoperan con los sistemas y aplicativos ubicados en los Centros de datos centralizados o con organismos terceros, incluyendo el "Punto Neutro".
- Memorias técnicas de los cambios realizados en los componentes con motivo de mejoras en el desempeño de los mismos o bien como resultado de la atención a incidentes, problemas, cambios.
- Memorias técnicas de la solución a incidentes y base de datos de errores conocidos.
- Base de Datos de Administración de Configuraciones.
- Memorias técnicas de los procesos de migración.
- Información, memorias, configuraciones o cualquier activo requerido por el Instituto definido en las mesas de trabajo semanales.

El **LICITANTE** deberá brindar acceso al Instituto a las bases del conocimiento relacionado con los servicios y entregar copia de dichas bases de conocimiento en medio electrónico cada mes, junto con los trámites de facturación correspondientes.

El **LICITANTE** deberá efectuar la transferencia de conocimiento, en los cuales personal del **LICITANTE** compartirá a personal del IMSS todo lo relacionado a la gestión de la operación y soporte de la infraestructura y servicios.

Actualización Tecnológica para Contenedores (Microservicios)

El **LICITANTE** deberá participar en conjunto con el Instituto en la definición y ejecución de la estrategia de migración que habilite el consumo de Contenedores (Microservicios) durante la vigencia del servicio.

El Instituto requiere efectuar acciones para que el 33% de los servicios Institucionales del ecosistema aplicativo sea susceptible de contenerizar a microservicios. Por ello de manera conjunta, el Instituto y el **LICITANTE** deberán contar con las capacidades necesarias en

algún(os) servicios, sistemas o aplicativos Institucionales, así como entregar un análisis e informe detallado del evento (Postmortem) a las 48 horas después de concluido el incidente. 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 de toda la información que se desprenda del presente anexo técnico. El **LICITANTE** deberá exponer y explicar el contenido de dicho repositorio al Instituto, así mismo habilitará accesos a dicho repositorio para los miembros del GGC. Al término del contrato, el **LICITANTE** transferirá al Instituto toda la información de dicho repositorio.

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 GGC del Instituto mensualmente 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 GGC 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 GGC 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 GGC 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, presentará al GGC de manera mensual 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 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 infraestructura 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.

ANEXOS
DIVISIÓN DE CONTRATOS

términos de recursos humanos, procesos de operación e infraestructura de TI para colaborar en el cumplimiento de esta estrategia y lograr la transformación y modernización de los servicios tecnológicos que el IMSS ofrece a sus derechohabientes y al público en general.
De manera conjunta, el Instituto y el **LICITANTE** deberán definir un modelo de gobierno para la actualización a contenedores (microservicios) que incluya de manera enunciativa más no limitativa: Esquemas de desarrollo, Políticas de Operación, Procesos, Métricas y Desempeño que regirán la forma de trabajar en los distintos proyectos que requieran ser administrados con una cultura de Integración Continua y Desarrollo Continuo para la migración a contenedores (microservicios) incluyendo el manejo y operación del pipeline.

De manera conjunta, el Instituto y el **LICITANTE** deberán definir arquitecturas operativas, las cuales deberán ser notificadas a las distintas áreas técnicas del Instituto, a fin de que sean atendidas y utilizadas por las distintas fábricas de software y áreas de desarrollo del Instituto.

Grupo de Gobierno del Contrato

El Grupo de Gobierno del Contrato estará conformado por los responsables de los siguientes servicios:

Servicio	Integrantes
Servicio de Continuidad Operativa y Soporte a la Operación	Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional Titular de la Coordinación Técnica de Administración de Centro de Datos Titular de la División de Administración de Centros de Datos.
Servicio de Continuidad y Soporte de Telecomunicaciones	Titular de la Coordinación Técnica de Telecomunicaciones
Servicio de Continuidad y Soporte de Seguridad	Titular de División de Seguridad Informática

Los miembros del Grupo de Gobierno del Contrato (GGC) 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, cambios, eventos, problemas, y cualquier información relacionada al servicio prestado.
El **LICITANTE** deberá de efectuar e informar mensualmente al GGC del Instituto el seguimiento de cada servicio, informando avances, estado de requerimientos, asuntos, consumos, riesgos, desviaciones, incidentes, cambios, eventos, problemas e información relacionada al servicio prestado tales como: memorias técnicas de instalación configuración y puesta a punto de los aplicativos, ejercicio presupuestal detallado por servicio, infraestructura, proyección del gasto, aplicativo, planes de actualización tecnológica, arquitectura por aplicativo, CMDB, detalle del licenciamiento instalado y distribución por aplicativo, fechas de vencimiento de los certificados, proyección de crecimiento por aplicativo, capacidad de la infraestructura y memorias técnicas de las migraciones ejecutadas al inicio y durante la vigencia del servicio.
El **LICITANTE** deberá avisar de manera inmediata al responsable del GCC del servicio afectado, al momento de presentarse un evento o incidente que afecte la operación de

El IMSS en caso de contar con contratos de licenciamientos con distintos fabricantes (base de datos, sistema operativo o licenciamientos diversos), proporcionará al **LICITANTE** los datos requeridos para que el **LICITANTE** a nombre del IMSS levante los tickets que en su caso se requieran a fin de solventar incidencias, eventos o actualizaciones. En el caso de que el Instituto no cuente con contratos de licenciamiento o en que esos contratos no sean suficientes para atender las necesidades institucionales, el Instituto podrá solicitar al **LICITANTE** que habilite el licenciamiento correspondiente en la modalidad de servicio administrado. Preferentemente se buscará utilizar los contratos de licenciamiento del IMSS.

El LICITANTE definirá e implementará mecanismos de comunicación hacia los responsables de 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.

El **LICITANTE** elaborará en un plazo no mayor a 10 días hábiles posteriores a la adjudicación del contrato, una matriz de los verbos, sujetos obligados, 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".

El **LICITANTE** a partir de la matriz de verbos, deberá generar 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 habilitado por el **LICITANTE** con acceso permanente a los administradores del contrato (grupo de gobierno del contrato) y deberá actualizarse, y presentarse de manera mensual en las juntas de gobierno del contrato.

5. Pruebas

No se requiere la ejecución de procesos de prueba durante el procedimiento de contratación.

6. Perfil del Proveedor

El **LICITANTE** deberá cumplir con las siguientes certificaciones de Centros de Datos así como, de Gestión del Servicio que se listan de manera enunciativa más no limitativa en la siguiente tabla:

Componente o Servicio	Descripción	Especificación	Tipo
Certificación de Centros de Datos	Certificación de Disponibilidad del Centro de Datos Ofertado	TIER III o ICREA IV equivalente o superior	Funcional
Gestión de Servicios de Tecnologías de la Información y	Certificación de gestión de procesos de Tecnologías de la Información y Comunicaciones.	ITIL V3 equivalente o superior	Funcional

ANEXOS
DIVISIÓN DE CONTRATOS

Componente o Servicio	Descripción	Especificación	Tipo
Comunicaciones			
Sistemas de Gestión del Servicio	Calidad en la Gestión de Servicios de TIC	ISO/IEC 20000-1 equivalente o superior	Funcional
Gestión de Seguridad de la Información	Implementación, Mantenimiento y gestión de Sistemas de Gestión de Seguridad de la Información	ISO 27001 equivalente o superior	Funcional

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 de al menos 5 años para brindar los servicios objeto del presente anexo técnico, apéndices, así como términos y condiciones, para lo cual deberá de presentar copia de contratos, pedidos o convenios formalizados con el sector público o privado cuyo objeto esté relacionado con los servicios de la presente licitación.

El **LICITANTE** deberá contar con especialidad comprobable con al menos 5 contratos formalizados cuyo objeto esté relacionado con la prestación de servicios similares al de la presente licitación.

Certificaciones enunciativas más no limitativas, o en su caso, similares en funcionalidad o tema en:

- **ISO/IEC 27001**
- **ISO/IEC 20000**
- **ITIL Expert Certificate**
- **ITIL Foundation Certificate in IT Service Management**
- **ITIL intermediate in Operational support and analysis**
- **ITIL intermediate in Service Offering AND Agreements**
- **ITIL intermediate un Release, control and validación**

El Administrador de proyectos deberá contar con las siguientes certificaciones:

- **Project Management Institute (PMI)**
- **ITIL Foundation Certificate in IT Service Management version 4**
- **Scrum Certified Master**

El **LICITANTE** deberá contar con el personal certificado en Metodologías de Administración de Proyectos para la dirección del proyecto.

El **LICITANTE** deberá contar con el personal certificado o con experiencia comprobable en productos, software y componentes descritos en el presente anexo técnico por lo que deberá adjuntar a su propuesta las siguientes certificaciones:

- CCNA - Cisco Certified Network Associate
- CCNA - Cisco Certified Network Associate Routing and Switching
- CCNP - Cisco Certified Network Professional
- Cisco Certified Specialist - Data Center Core
- CISM - Certified Information Security Manager
- CISSP Certified Information Systems Security Professional
- MCITP Enterprise Administrator on Windows Server 2008
- MCTS Microsoft Exchange Server 2007 Configuration
- Scrum Master Certified Credential
- Exchange Server 2007 Configuration
- Windows Server 2008 Active Directory, Configuring
- Windows Server 2008 Applications Infrastructure, Configuring
- Windows Server 2008 Network Infrastructure, Configuring
- Windows Server 2008, Enterprise Administrator
- Microsoft SQL Server 2008, Implementation and Maintenance
- Oracle Certified Associate - Oracle WebLogic Server 11g System Administrator
- Oracle Database 11g: Administrator Certified Associate
- Oracle Database 11g: Administrator Certified Professional
- Oracle Database 12c Certified Implementation Specialist
- Oracle WebLogic Server 12c Administrator
- Oracle VM 3.0 for x86 Certified Implementation Specialist
- VMware Certified Professional Data Center Virtualization 2019 o superior
- Querying Microsoft SQL Server 2012/2014 o superior
- Administering Microsoft SQL Server 2012/2014 Databases
- Implementing a Data Warehouse with Microsoft SQL Server 2012/2014
- Microsoft Certified Solutions Associate SQL Server 2012/2014
- Red Hat Certified System Administrator Enterprise Linux 6 o superior

El **INSTITUTO** podrá solicitar en cualquier momento del proceso de contratación y durante la vigencia del contrato, los originales de las certificaciones presentadas por el **LICITANTE** para su cotejo, mismas que serán devueltas una vez concluida la revisión.

El **LICITANTE** deberá presentar al Instituto, a través de la Coordinación de Servicios de Infraestructura Tecnológica Institucional cita en Toledo 21 6to piso, 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 de 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, el plan de trabajo, 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

ANEXOS
DIVISIÓN DE CONTRATOS

TIC acorde a lo descrito en el anexo técnico y con los que el Instituto estará colaborando, su cargo y puesto así como los datos y la vía de comunicación para contactarlo.

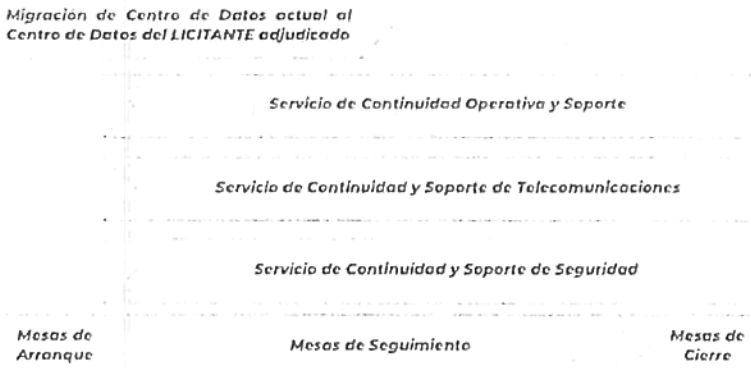
7. Condiciones técnicas de aceptación de entregables

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.

8. Cronograma de actividades

El **LICITANTE** deberá entregar el plan de trabajo estableciendo actividades, responsables, tiempos para dar cumplimiento de las obligaciones relacionadas a los servicios del presente anexo técnico.

La siguiente imagen se mencionan las etapas principales del plan de trabajo que incluye:



Etapas del servicio

El **LICITANTE** en su propuesta deberá incluir el Plan de Trabajo especificando de manera detallada hitos y fases para el cumplimiento de cada una de las etapas y servicios objeto del presente anexo técnico. El plan de trabajo presentado por el **LICITANTE** adjudicado, debera integrar informació n a detalle para los servicios siguientes:

- Servicio de Continuidad Operativa y Soporte
- Servicio de Continuidad y Soporte de Telecomunicaciones
- Servicio de Continuidad y Soporte de Seguridad

El **LICITANTE** adjudicado deberá incluir el detalle para la etapa de **Migración del Centro de Datos Actual al Centro de Datos ofertado** .

El plan de trabajo presentado por el **LICITANTE** deberá incluir el esfuezo de trabajo detallado de cada bloque de trabajo que integren los servicios, incluir duración de las etapas importantes dimensionando los tiempos de afectación, que permitan al Instituto evaluar técnica y funcionalmente la viabilidad del plan de trabajo.

A continuación, se especifica de manera enunciativa más no limitativa, los principales hitos, indicando fase, identificador, descripción del hito, las fechas relativas y absolutas de inicio y/o término y cantidad de días naturales máximos.

Tabla Hitos relevantes a considerar en el Plan de trabajo

Fase	ID	Hito	Inicio / Término Máximo del Hito	Máxima duración en días naturales*	Precedente(s)
Proceso de Migración de Centro de Datos actual al Centro de Datos ofertado por el **LICITANTE**.					
Planeación del Arranque	1	Kick-Off y presentación del equipo de trabajo del **LICITANTE**.	A más tardar 3 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	A más tardar 5 días naturales posteriores al Fallo	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 de arranque.	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 3 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	A lo largo de los siguientes 25 días naturales a partir del Kick-Off del proyecto	Plazo ofertado por el posible **LICITANTE**	1

ANEXOS
DIVISIÓN DE CONTRATOS

Fase	ID	Hito	Inicio / Término Máximo del Hito	Máxima duración en días naturales*	Precedente(s)
		Terceros Involucrados en los servicios del presente anexo técnico.			
Actividades de migración de centro de datos actual al centro de datos del **LICITANTE** adjudicado.	6	Inicio de actividades de migración del centro de datos actual al centro de datos ofertado por el **LICITANTE** incluyendo servicios de punto neutro y todo lo necesario para la operación de los servicios.	Al día natural siguiente a la aprobación, por parte del IMSS, del Plan de Trabajo Detallado	Plazo ofertado por el posible **LICITANTE**	4
	7	Estrategia de continuidad de servicios del Centro de Datos Actual durante el proceso de migración al centro de Datos ofertado por el **LICITANTE**.	Al día natural siguiente a la aprobación, por parte del IMSS, del Plan de Trabajo Detallado	Plazo ofertado por el posible **LICITANTE**	4
	8	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
	9	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
	10	Inicio de los Servicios asociados a la continuidad operativa de los servicios del presente anexo	Plazo ofertado por el posible **LICITANTE**	Plazo ofertado por el posible **LICITANTE**	N/A

Fase	ID	Hito	Inicio / Término Máximo del Hito	Máxima duración en días naturales*	Precedente(s)
		técnico.			
	11	Inicio de actividades de migración tecnológica hacia ambientes basados en contenedores	Plazo ofertado por el posible **LICITANTE**	Plazo ofertado por el posible **LICITANTE**	8
	12	Habilitación de ambientes en los Centros de Datos designados por el Instituto.	Plazo ofertado por el posible **LICITANTE**	Plazo ofertado por el posible **LICITANTE**	8
	13	Actividades de Finalización del Contrato.	A más tardar 4 meses naturales antes del día de la Finalización del Contrato	31 de diciembre de 2022	N/A
CIERRE	14	Finalización del Contrato	-	31 de diciembre de 2022	N/A

9. Niveles de servicio acordados que deberán cumplirse

El **LICIANTE** deberá cumplir el nivel de servicio requerido para los servicios de infraestructura de procesamiento, almacenamiento, respaldos, telecomunicaciones y seguridad, incluyendo aplicaciones, componentes, servicios digitales y todos elementos necesarios para su funcionamiento, conforme a la siguiente tabla:

Nivel de Disponibilidad	**Minutos indisponibles permitidos en el mes para los servicios del presente contrato** **A partir de este límite se aplicarán deductivas por prestación deficiente del servicio**
99.982%	7.8 minutos

El **LICITANTE** deberá habilitar, instalar, configurar, poner a punto y operar una solución ó herramienta para medir los diferentes niveles de servicio de la infraestructura de procesamiento, almacenamiento, respaldos, telecomunicaciones y seguridad, incluyendo todos elementos necesarios para su funcionamiento. El **LICITANTE** debe utilizar las herramientas habilitadas en el **Servicio de Continuidad a la Operación y Soporte** como entrada de datos, así como

ANEXOS
DIVISIÓN DE CONTRATOS

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.

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.

El **LICITANTE** proporcionará la transferencia de conocimiento y adiestramiento tecnológico necesario en el manejo y administración de las herramientas de niveles de servicio para el personal definido por el Grupo de Gobierno del Contrato, 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 y las mesas de trabajo semanales.

El software para niveles de servicio propuesto por el **LICITANTE** 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
- 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

9.1. Definición General de Entrega

El **LICITANTE** deberá dar cumplimiento a la entrega de los servicios acorde a las especificaciones, condiciones, tiempos de entrega definidos en el presente anexo, los servicios entregados serán validos por el Instituto cuando 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 específica, dedicada a los diferentes servicios del presente anexo técnico.

9.2. 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 y fecha de entrega máxima a partir de la cual se aplicarán deductivas	Inicio de la Entrega
Reporte de Entrega del Servicio			
01	**Disponibilidad de los aplicativos**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
02	**Utilización y desempeño de la infraestructura**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
03	**Impacto a la operación en tiempo (minutos)**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
04	**Reporte de Gestión de Requerimientos**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
05	**Reporte de Gestión de Incidentes**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
06	**Reporte de Gestión de Problemas**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
07	**Reporte de Gestión de Configuraciones**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
08	**Reporte de Gestión de Cambios**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio

ANEXOS
DIVISIÓN DE CONTRATOS

Num.	Nombre y Descripción	Frecuencia del reporte y fecha de entrega máxima a partir de la cual se aplicarán deductivas	Inicio de la Entrega
09	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

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:

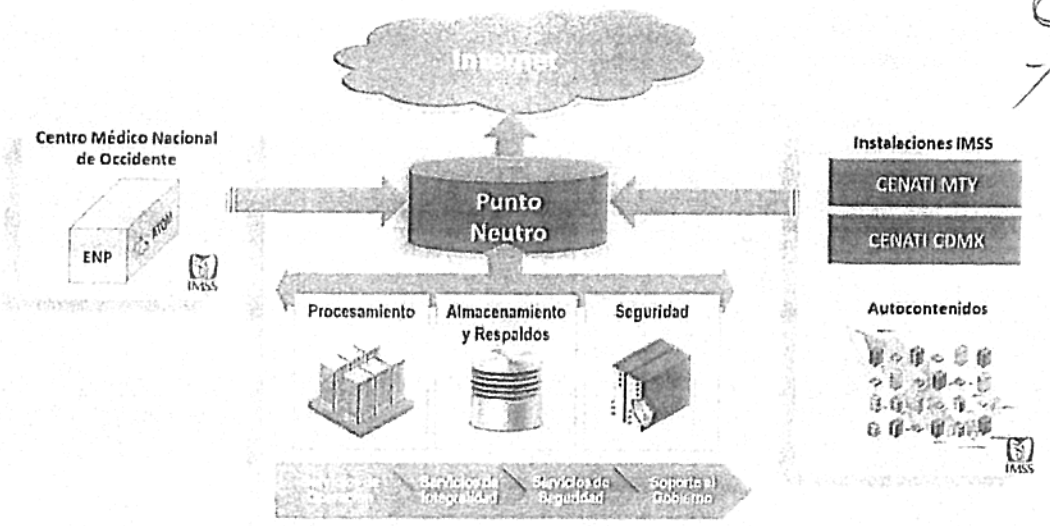
- Mes que se evalúa
- Cantidad total de acciones realizadas en el mes
- Cantidad total de acciones realizadas dentro de la ventana de tiempo establecida en el mes
- Anexo de relación de acciones realizadas, identificando su tipo, tiempo de inicio y finalización
- Valores esperados en el mes para cada 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.

9.3. 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.

10. Requerimientos de arquitectura tecnológica

El modelo actual del ecosistema del Instituto con el cual se brindan los servicios a sus derechohabientes, patrones, jubilados, pensionado y público en general se muestra a continuación de manera conceptual:



ANEXOS
DIVISIÓN DE CONTRATOS

El proveedor deberá considerar en su propuesta técnica la complejidad del ecosistema que se ha construido bajo el concepto de arquitectura empresarial por lo menos en los 8 últimos años, Como se puede observar en la imagen anterior, los dominios tecnológicos que lo integran con más de 98,000 componentes de configuración atienden las diferentes necesidades operativas del Instituto y su interacción.

El criterio para considerar concluida la migración desde el Centro de Datos actual hacia el Centro de Datos ofertado, será en el momento en que se encuentren los servicios descritos anteriormente activos y operando en la infraestructura propuesta por el Licitante, e interactuando con el ecosistema tecnológico institucional, esto es; con los ambientes operativos digitales productivos y no productivos instalados en los diferentes centros de datos IMSS y del Gobierno Federal así como organismos con los que interactúa el Instituto tales como SAT, RENAPO, INFONAVIT, BANCO DE MÉXICO, PROCESAR, CONSAR, BANCOS Y AFORES, entre otros, validados de conformidad por el personal que el Instituto designe (áreas de telecomunicaciones y seguridad informática, infraestructura tecnológica, desarrollo, monitoreo así como el personal de las direcciones normativas que hacen uso de los servicios en los casos que aplique).

Por lo anterior el Licitante adjudicado deberá realizar actividades técnicas complejas para migrar los servicios, aplicaciones y demás componentes al Centro de Datos propuesto incorporando en su modelo arquitectónico los elementos que garanticen la continuidad operativa del Instituto, los elementos de análisis para arquitectar la solución propuesta se encuentran en los apéndices "Componentes de Infraestructura" y "Apéndice Detalle de Servicios."

Asimismo, el Licitante deberá considerar en su propuesta técnica los lineamientos establecidos en el ~~acuerdo para~~ ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, emitido por la Coordinación de Estrategia Digital Nacional, el pasado mes de septiembre de 2021.

11. Restricciones e interfaces con otros elementos

El Centro de Datos actual intercambia información y ejecuta diversos procesos con diferentes ecosistemas y entidades privadas y públicas, tales como:

- Centros Nacional de Tecnologías de Información propiedad del Instituto (CENATI).
- Centro de Datos de Gobierno Federal en el Instituto Potosino de Investigación Científica y Tecnológica (IPICYT).
- Entidades externas (tales como: SAT, RENAPO, Procesar, Banco de México, INFONAVIT, Bancos, Instituto Nacional Electoral, Afores, CONSAR, entre otros)

Intercambio de información que el Instituto tiene de manera enunciativa mas no limitativa, son las siguientes:

Para el caso del Centro Nacional de Tecnologías de Información en Monterrey, se intercambia información de manera diaria para la actualización de información relacionada a asegurados, patrones, pensiones, para alimentar los procesos de Afiliación, Recaudación e Incorporación, así como Prestaciones económicas y Sociales.

Respecto al Instituto Potosino de Investigación Científica y Tecnológica, se tiene un modelo de intercambio de información entre las aplicaciones que se han desplegado en el centro de datos de

gobierno federal y el centro de datos actual, para el consumo de servicios de vigencia de derechos, firma electrónica, bóveda y servicios transversales por parte de las aplicaciones que dan atención a la pandemia por COVID19, así como esquemas de replicación de bases de datos para las bases de datos de vacunas, vigilancia epidemiológica y base de datos transaccional única.

Finalmente para las entidades externas públicas o privadas, el centro de datos actual, tiene interconexión con los centros de datos propios del Instituto o del Gobierno Federal y entidades externas (tales como: SAT, RENAPO, Procesar, Banco de México, INFONAVIT, Bancos, Instituto Nacional Electoral, Afores, CONSAR, entre otros) para el intercambio de información, conforme a los estándares de telecomunicaciones y seguridad definidos por el Instituto.

12. Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Héctor Javier Reyes Oropeza	Titular de la División de Administración de Centros de Datos.		06/05/2022

Revisó	Cargo	Firma	Fecha
Javier cortés López	Titular de la Coordinación Técnica de Operación y Administración de Centro de Datos		06/05/2022

Aprobó	Cargo	Firma	Fecha
Eduardo Oropeza Ortiz	Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional		06/05/2022

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

Apéndice 1

Componentes de Infraestructura

SGMP_Apéndice_1

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

ANEXOS
DIVISIÓN DE CONTRATOS

Contenido

1 Objetivo del Documento 4
2 Infraestructura 4
2.1 Plataforma 4
2.1.1 Hardware 4
2.1.2 Sistema Operativo 14
2.1.3 Plataformas de virtualización 15
2.1.4 Virtualización 18
2.2 Red 19
2.2.1 Zona 19
2.2.2 Pública 25
2.2.3 Infraestructura de Red 27
2.3 Instalaciones 28
2.3.1 Co-ubicación en modalidades de despliegue 28
3 Aplicaciones 29
3.1 Análisis estadístico 29
3.1.1 Sistema de gestión de bases de datos 29
3.2 Herramientas y entorno de desarrollo 30
3.2.1 Entorno de desarrollo integrado (IDE) 30
3.2.2 Gestión de documentos y contenidos 31
3.3 Middleware 32
3.3.1 Bus de servicios empresariales (ESB) 32
3.4 Comunicación unificada y colaboración 33
3.4.1 Correo electrónico 33
4 Operación Digital 36
4.1 Servicios Generales 36
4.1.1 Gestión de la seguridad cibernética 36
4.1.2 Soporte para la entrega de servicios institucionales 36
4.1.3 Infraestructura Web 36
5 Firmas de elaboración, revisión y aprobación 37

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	07/12/2021	Elaboración del documento	Héctor Javier Reyes Oropeza
0.2	07/12/2021	Revisión del documento	Javier Cortés López
0.3	07/03/2022	Actualización del documento	Héctor Javier Reyes Oropeza
0.4	06/05/2022	Actualización del documento	Héctor Javier Reyes Oropeza
1.0	06/05/2022	Aprobación del documento	Eduardo Oropeza Ortiz

ANEXOS
DIVISIÓN DE CONTRATOS

1 Objetivo del Documento

El objetivo del presente Apéndice es establecer la descripción de los Componentes de Infraestructura referidos en el Anexo Técnico del Servicio Administrado objeto de esta Licitación.

2 Infraestructura
2.1 Plataforma
2.1.1 Hardware
2.1.1.1 Servidores de medio desempeño
2.1.1.1.1 Servidor X86 Modalidades CDP, ENP y SDI

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

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

Los soportes para los sistemas operativos Oracle y Windows serán proporcionados por el Instituto, el Licitante deberá integrar en su propuesta el licenciamiento así como el soporte para los productos Linux.

2.1.1.1.2 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

ANEXOS
DIVISIÓN DE CONTRATOS

- Protección anti-tampering de la tarjeta HSM (sensores al menos para temperatura, acceso físico, tensión)
- Generación de números aleatorios por hardware
- Puertos Gigabit Ethernet

2.1.1.2 Medios de almacenamiento de acceso directo

2.1.1.2.1 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

2.1.1.2.2 Respaldo de Datos Individual

Se requiere el servicio para el sistema de respaldos de Datos con las siguientes características:

- 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

ANEXOS
DIVISIÓN DE CONTRATOS

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.

2.1.1.2.3 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 asíncrono, 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 tecnología integrada para la optimización del almacenamiento mediante la compresión y deduplicación a nivel de bloque
- Software o tecnología 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.

2.1.1.2.4 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 6
- 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 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 respaldos debe ser "en línea", esto es, no debe realizarse en un proceso posterior.

ANEXOS
DIVISIÓN DE CONTRATOS

- 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.

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 6.

2.1.1.2.5 Unidad de Respaldo en Cintas

- Deberá proveer la infraestructura para la realización de respaldos y restauraciones de información. El proveedor deberá incluir el hardware, software y soporte para realizar los respaldos y restauraciones.
- La librería no deberá tener anuncio de fin de vida y contar con al menos las capacidades solicitadas.
- La librería será dedicada y de uso exclusivo para el Instituto.
- Como parte de la infraestructura se deberá contemplar al menos un servidor para la consola de respaldos en plataforma UNIX , LINUX o WINDOWS, que realice respaldos a disco, cinta virtual o cinta física, así como el manejo de librerías físicas y virtuales.
- La solución de respaldos deberá enviar la información a disco y posteriormente a cinta, para ello se ocuparán los BCFs correspondientes y de acuerdo con la vigencia y/o uso de la información, estas pasarán a respaldarse en cinta como información histórica.
- El proveedor en conjunto con el Instituto acordará las políticas de respaldo y retención, las cuales podrán ser actualizadas de común acuerdo con **El LICITANTE**, para una mejor operación.

- La solución propuesta deberá tener capacidad de deduplicación y utilizar la última y/o penúltima versión liberada, de la herramienta de respaldos.
- La solución de respaldos deberá tener la capacidad de realizar respaldos totales, incrementales, diferenciales y/o consolidados.
- Deberá contar con un monitoreo, donde se pueda ver el estatus de los respaldos y generar notificaciones automáticas de respaldos fallidos, por ejemplo, vía correo electrónico, preferentemente deberá integrarse con la herramienta de Monitoreo propuesta.
- La solución de respaldos deberá permitir navegar por los objetos respaldados (archivos y directorios) y a partir de ahí, seleccionar la información que se desea recuperar, la información a restaurar deberá ser mostrada de forma similar a la de un explorador de Windows, permitiendo la navegación por los diferentes niveles de los objetos a restaurar.
- La solución de respaldos deberá permitir ejecutar respaldos y recuperaciones de manera calendarizada, para verificar la integridad física y lógica de los respaldos con el objeto de asegurar que los datos fueron correctamente grabados.
- La solución de respaldos deberá permitir asignar distintas políticas de retención, las cuales dependen del tipo de información, el medio de almacenamiento y la fecha de realización del respaldo, cuando se requiera tener una expiración indefinida para un respaldo, se debe permitir el manejo de archivado y su restauración al ser requerido.
- La solución de respaldos deberá permitir la restauración de información en servidores diferentes al origen del respaldo.
- La solución de respaldos ofertada deberá soportar la integración con soluciones de virtualización.
- Deberá proporcionar la plataforma respaldos en Cintas para el Centro de Datos Principal y deberá contar con al menos las siguientes características técnicas.
    - 4 Drives LTO8 con un total de 100 slots
    - Contar con un sistema de respaldo en cinta al menos LTO-8.
    - Las cintas LTO-8 necesarias para mantener la operación durante la vigencia del contrato, serán solicitadas en su BCF correspondiente.
    - Deberá proporcionar el licenciamiento necesario para encriptación y administración, sin costo para el Instituto.

Las cintas deberán ser resguardadas como parte del servicio entregado por El LICITANTE y el precio unitario ofertado para ejercer su resguardo estará asociado a paquetes de 50 cintas por unidad.

2.1.1.2.6 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 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)

ANEXOS
DIVISIÓN DE CONTRATOS

- 10 GbE: 2 de 10 GbE (SRDF)
- Permitir la configuración de por lo menos los siguientes RAID:
  - .
  - RAID 5: (3 + 1) o (7 +1) para todas las unidades.
- Ser compatible con la plataforma Mainframe.

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 o superior.

2.1.1.3 Medios de almacenamiento extraíbles

2.1.1.3.1 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

ANEXOS
DIVISIÓN DE CONTRATOS

2.1.2 Sistema Operativo

2.1.2.1 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 componentes de infraestructura 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 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

2.1.2.1.3 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:

- Hacer uso de la subscripción de soporte de ORACLE SERVER LINUX (6 o superior) o equivalente (soporte empresarial 7/24 en línea y presencial a través del

contrato de licenciamiento y soporte que tiene contratado el Instituto con el fabricante, 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 a través del contrato de soporte y licenciamiento con el que cuenta el Instituto con Oracle
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

2.1.3 Plataformas de virtualización

2.1.3.1 Servidores

2.1.3.1.1 Servidor virtual RISC Modalidad CDP, ENP y SDI

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
  - 8 threads por procesador

Y deberá ser escalable con al menos incrementos de:

- Módulos de 1 core con 8 threads por core

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:

- 5puertos 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

ANEXOS
DIVISIÓN DE CONTRATOS

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 *

* Más actualización de parches

2.1.3.1.2 Servidor virtual X86 Modalidades CDP, ENP y SDI

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 de procesador físico
  - Capacidad base de 4 vCPUs de procesador virtual

Y deberá ser escalable con al menos incrementos de:

- Módulos de 4 vCPUs

La memora RAM BASE deberá ser cuando menos de:

- 16 GB de memoria RAM

Incremento de 8 GB de memoria RAM Servidores virtuales 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 8 GB de memoria que oferta el Proveedor.

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

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 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 2012 / 2014 Server o superior
- Diferentes Distribuciones Linux

2.1.3.2 Entorno para el usuario final

2.1.3.2.1 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
- Puerto de red Ethernet
- 6 Puertos USB
- Mouse óptico de 2 botones
- Teclado en español
- Monitor de 19 pulgadas como mínimo

2.1.3.2.2 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

ANEXOS
DIVISIÓN DE CONTRATOS

2.1.4 Virtualización

2.1.4.1 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, las cuales deberán dar continuidad a las que hoy en día tiene el Instituto en operación: VMWare, OVM y KVM

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, con capacidad de soportar hasta 800 cores por Plataforma.

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. Las nuevas deberán soportar los últimos sistemas operativos liberados por el fabricante del mismo.
- 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, cuando sea requerido por el Instituto y 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.

2.2 Red
2.2.1 Zona
2.2.1.1 Punto Neutro

El Instituto requiere establecer comunicación desde diferentes ubicaciones o localidades remotas hacia el centro de datos ofertado, donde podrán converger 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 través 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:

- Deberá incluir Interfaces Físicas 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.
  - Flexibilidad de manejo de tráfico con la configuración de clases de servicio sobre el tráfico de WAN público y WAN privado.
  - 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.

ANEXOS
DIVISIÓN DE CONTRATOS

- Capacidad para recibir al menos 100 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 al menos 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:

• 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.

2.2.1.1.1 Red de Área Amplia (WAN)

Para Punto Neutro la Red de Área 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 tráfico 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 críticas.
- 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.

2.2.1.1.2 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.

ANEXOS
DIVISIÓN DE CONTRATOS

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 podrán ser solicitados a través del consumo de los BCFs correspondientes, pues se entiende que forman parte de la arquitectura integral del servicio solicitado por el 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.

2.2.1.1.3 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, redireccionándolos hacia los destinos correspondientes.

Deberá considerar el 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 integra, 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 y notificación de Red y Abusos mediante un Noc y SOC respectivamente a través del proceso de Gestión de Eventos.
- 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.
- Capacidad de integrar 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 necesarios para la entrega de los servicios descritos en el presente Anexo Técnico.
Deberá generar reportes de capacidad de infraestructura de datos para el crecimiento con las menores afectaciones a la operación.

2.2.1.1.4 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, redireccionándolos hacia los destinos correspondientes.

ANEXOS
DIVISIÓN DE CONTRATOS

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 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.
- 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.

2.2.1.1.5 **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.

2.2.2 Pública

2.2.2.1 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 considerar la integración de 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

2.2.2.1.1 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.

ANEXOS
DIVISIÓN DE CONTRATOS

- 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.

2.2.2.1.2 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% aplicable sobre la falla de ambos enlaces.
- 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.
- 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.

2.2.3 Infraestructura de Red
2.2.3.1 Virtualización de redes
2.2.3.1.1 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

ANEXOS
DIVISIÓN DE CONTRATOS

- 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
2.3.1.1 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 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.

2.3.1.2 Modalidades de co-ubicación
2.3.1.2.1 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.

2.3.1.2.2 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 Análisis estadístico

3.1.1 Sistema de gestión de bases de datos

3.1.1.1 Subscripciones a Bases de Datos Open Source

El Instituto podrá solicitar al proveedor la suscripción al uso de Bases de Datos Open Source.

ANEXOS
DIVISIÓN DE CONTRATOS

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 como:
  - Stanalone
  - Cluster (HA)

- El proveedor deberá considerar al menos las siguientes plataformas de Base de Datos opencource: PostgreSQL, MySQL, Maria DB, Berkeley DB (con licencia GNU AGPL), Cassandra DB, Mongo DB y Hadoop.
- 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.
- Arrancar o levantar 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 OpenSource 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 Herramientas y entorno de desarrollo

3.2.1 Entorno de desarrollo integrado (IDE)

3.2.1.1 Kit de Desarrollo de Software (SDK)

3.2.1.1.1 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 haciendo uso del acuerdo de Licenciamiento y soporte suscrito entre el Instituto y el fabricante.

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

3.2.2 Gestión de documentos y contenidos

3.2.2.1 Gestión de contenidos Web

3.2.2.1.1 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

3.2.2.1.2 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

ANEXOS
DIVISIÓN DE CONTRATOS

3.2.2.1.3 Alfresco

El Instituto requiere de servicios de para gestión de contenido Alfresco a través de una plataforma integrada que brinde servicios, repositorios, API, soluciones y herramientas de procesamiento empresarial centrados en el contenido para promover la transformación digital. La plataforma Alfresco debe contar con las siguientes funcionalidades:

- gestión de documentos,
- procesos de back-office,
- aplicaciones de procesos de negocio,
- gestión de registros
- productividad del equipo.

La plataforma de gestión de contenido debe permitir la creación de un repositorio propio. Los servicios y datos deberán integrarse con aplicaciones y repositorios externos no nativos a través de conectores prediseñados, desarrollo de API o integraciones.

La plataforma debe ofrecer interfaz de aplicaciones web que permita a los usuarios navegar y trabajar con los diferentes servicios de contenido. La plataforma debe ofrecer soluciones prediseñadas para procesos de contenido verticales y horizontales.

El licenciamiento será por core o por nodo de acuerdo al esquema definido por el fabricante.

3.3 Middleware
3.3.1 Bus de servicios empresariales (ESB)
3.3.1.1 Software de mensajería
3.3.1.1.1 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), haciendo uso del Licenciamiento y soporte provisto por el Instituto.
- Versión del producto 9.2 y posteriores
- Soporte del producto por 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

3.3.1.1.2 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

3.3.1.1.3 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

3.3.1.1.4 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

3.4 Comunicación unificada y colaboración

3.4.1 Correo electrónico

3.4.1.1 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

ANEXOS
DIVISIÓN DE CONTRATOS

- 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:

Perfil de Usuarios	Cuota de Buzón en MB	% de Usuarios por perfil
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.

Respaldos, Restauración y Depuración de la Información

El Proveedor deberá establecer un esquema de respaldos en línea, restauración y depuración 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, los mensuales de 3 meses.y el anual 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

Protección en el correo electrónico

- 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.

ANEXOS
DIVISIÓN DE CONTRATOS

4 Operación Digital
4.1 Servicios Generales
4.1.1 Gestión de la seguridad cibernética
4.1.1.1 Identificación y autenticación
4.1.1.1.1 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

4.1.2 Soporte para la entrega de servicios institucionales
4.1.3 Infraestructura Web
4.1.3.1.1 Solución para el cumplimiento WCAG

Los Web Content Accessibility Guidelines (Directrices de Accesibilidad para el Contenido Web, WCAG por sus siglas en inglés) son una parte de las directrices de accesibilidad web publicados por la Web Accessibility Initiative (Iniciativa de Accesibilidad Web, WAI) parte del World Wide Web Consortium (W3C), la principal organización de estándares de internet.

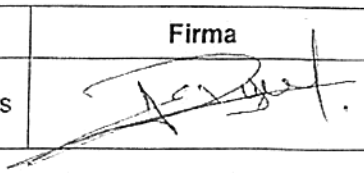
Son un conjunto de directrices que especifican cómo hacer el contenido web más accesible, especialmente a personas con discapacidades. La versión actual de estas directrices es la WCAG 2.0, publicado en diciembre de 2008 y convertido en estándar ISO/IEC 40500:2012 en octubre de 2012.

El Instituto requiere el servicio de Solución para el cumplimiento WCAG durante la vigencia del contrato con al menos las siguientes características:

- Plataforma que se pueda integrar al Portal Web del Instituto con una instalación tipo "one-line-code".
- Que cumpla con los estándares: WCAG 2.0, WCAG 2.1, ADA, Section 508.
- Lector de pantalla.
- Navegación por teclado.
- Bloqueo de parpadeo.
- Manejo de contraste y de colores.

- Manejo de tamaño de fuente.

5 Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Héctor Javier Reyes Oropeza	Titular de la División de Administración de Centros de Datos.		06/05/2022

Revisó	Cargo	Firma	Fecha
Javier cortés López	Titular de la Coordinación Técnica de Operación y Administración de Centro de Datos		06/05/2022

Aprobó	Cargo	Firma	Fecha
Eduardo Oropeza Ortiz	Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional		06/05/2022

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

Apéndice 2

Ubicaciones Geográficas

SGMP_Apéndice_2

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

ANEXOS
DIVISIÓN DE CONTRATOS

Contenido

1	Objetivo del Documento	4
2	Consideraciones geográficas de centro de datos primario	4
3	Ubicaciones iniciales de extensión de nube privada	4
4	Firmas de elaboración, revisión y aprobación	8

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	07/12/2021	Elaboración del documento	Héctor Javier Reyes Oropeza
0.2	07/12/2021	Revisión del documento	Javier Cortés López
0.3	21/12/2021	Actualización del documento	Héctor Javier Reyes Oropeza
0.3	07/03/2022	Actualización del documento	Héctor Javier Reyes Oropeza
0.4	06/05/2022	Actualización del documento	Héctor Javier Reyes Oropeza
1.0	06/05/2022	Aprobación del documento	Eduardo Oropeza Ortiz

ANEXOS
DIVISIÓN DE CONTRATOS

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.

De manera enunciativa mas no limitativa, 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.

- DELEGACIÓN CDMX NORTE - LA RAZA (5)
  - HE CMN La Raza: Calle Seris No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Ciudad de México.
  - HGO 3 CMN La Raza: Avenida Vallejo esq Antonio Valeriano No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Ciudad de México.
  - HI CMN La Raza: Circuito Interior Paseo de las Jacarandas No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Ciudad de México.

ANEXOS
DIVISIÓN DE CONTRATOS

- HG CMN La Raza: Circuito Interior Paseo de las Jacarandas No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Ciudad de México.
- BS CMN La Raza: Calle Seris No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Ciudad de México.

- DELEGACIÓN CDMX 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, Ciudad de México
  - 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, Ciudad de México

- DELEGACIÓN CDMX SUR - SXXI (5)
  - HE CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Ciudad de México.
  - HP CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Ciudad de México.
  - HC CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Ciudad de México.
  - HONCO CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Ciudad de México.
  - BS CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Ciudad de México.

- DELEGACIÓN CDMX 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, Ciudad de México.
  - HGZMF 8 San Ángel: Avenida Río Magdalena No. 289, Colonia Tizapán San Ángel C.P. 1090 Álvaro Obregón, Delegación Álvaro Obregón, Ciudad de México.

- 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:

- 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.

ANEXOS
DIVISIÓN DE CONTRATOS

4 Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Héctor Javier Reyes Oropeza	Titular de la División de Administración de Centros de Datos.		06/05/2022

Revisó	Cargo	Firma	Fecha
Javier cortés López	Titular de la Coordinación Técnica de Operación y Administración de Centro de Datos		06/05/2022

Aprobó	Cargo	Firma	Fecha
Eduardo Oropeza Ortiz	Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional		06/05/2022

Apéndice 3

Esfuerzos realizados para la migración de Centro de Datos Actual

SGMP_Apéndice_3

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

ANEXOS
DIVISIÓN DE CONTRATOS

Contenido

1	Objetivo del Documento	4
2	Tipos de Aplicaciones Institucionales	4
3	Complejidad de las Aplicaciones	4
4	Recursos Humanos	5
5	Calendarios de Migración	5
6	Tabla de esfuerzo de migración	5
7	Aplicaciones Migradas	7
8	Firmas de elaboración, revisión y aprobación	17

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	07/12/2021	Elaboración del documento	Héctor Javier Reyes Oropeza
0.2	07/12/2021	Revisión del documento	Javier Cortés López
0.3	07/03/2022	Actualización del documento	Héctor Javier Reyes Oropeza
0.4	06/05/2022	Actualización del documento	Héctor Javier Reyes Oropeza
1.0	06/05/2022	Aprobación del documento	Eduardo Oropeza Ortiz

ANEXOS
DIVISIÓN DE CONTRATOS

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	

ANEXOS
DIVISIÓN DE CONTRATOS

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

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
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	

ANEXOS
DIVISIÓN DE CONTRATOS

10	Alta Patronal Persona Fisica 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	

Apéndice 3 – Esfuerzos realizados para la migración de Centro de Datos Actual
Servicio de Continuidad de la Nube IMSS 2022

No.	Sistema	Área Usuaria	Tipo Aplicativo	Tipo Aplicativo	Esfuerzo (Días)
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 externo	Bajo	
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	

ANEXOS
DIVISIÓN DE CONTRATOS

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

No	Sistema	Área Usuaria	Tipo Aplicativo	Tipo Aplicativo	Esfuerzo en Días
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	
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

ANEXOS
DIVISIÓN DE CONTRATOS

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

No.	Sistema	Área Usuaria	Tipo Aplicativo	Tipo Aplicativo	Esfuerzo (HH)
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	Bajo	

ANEXOS
DIVISIÓN DE CONTRATOS

			centro de datos externo		
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

No	Sistema	Área Usuaria	Tipo Aplicativo	Tipo Aplicativo	# Subred
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	Mediano	

ANEXOS
DIVISIÓN DE CONTRATOS

			centro de datos 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 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 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
Héctor Javier Reyes Oropeza	Titular de la División de Administración de Centros de Datos.		06/05/2022

Revisó	Cargo	Firma	Fecha
Javier cortés López	Titular de la Coordinación Técnica de Operación y Administración de Centro de Datos		06/05/2022

Aprobó	Cargo	Firma	Fecha
Eduardo Oropeza Ortiz	Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional		06/05/2022

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

Apéndice 4

Relación actual de Infraestructura en Centro de Datos y proyección de crecimiento

SGMP_Apéndice_4

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

ANEXOS
DIVISIÓN DE CONTRATOS

Contenido

1 Objetivo del Documento 5
2 Relación actual de Infraestructura 5
3 Descripción de conceptos según servicio actual de Centro de Datos 7
3.1 Servidor X86 7
3.2 Módulo de Seguridad en Hardware (HSM) 7
3.3 Almacenamiento de Datos Individual 8
3.4 Respaldo de Datos Individual 8
3.5 Unidad de almacenamiento de media categoria para aplicaciones de bajo desempeño 8
3.6 Unidad de respaldo de plataforma abierta 8
3.7 Unidad de Almacenamiento de Datos de alto rendimiento y red SAN 8
3.8 Unidad individual de respaldos (Portatil) 9
3.9 Sistema Operativo Red Hat Enterprise Linux 9
3.10 Sistema Operativo SLES 9
3.11 Sistema Operativo Windows Server 2008 10
3.12 Sistema Operativo Windows 2012 10
3.13 Servidor Virtual RISC SPARC 10
3.14 Servidor Virtual X86 4VCPU 16 RAM 10
3.15 Puntos de Acceso a la Nube 11
3.16 Escritorio en la Nube 11
3.17 Plataforma de Virtualizacion multi-tecnologia 11
3.18 Punto Neutro 11
3.19 Enlaces para conectividad de Red de Área Amplia e Internet 12
3.20 Balanceador de carga de capas L4-L7 12
3.21 Plataforma Nodo de Extensión de Nube Privada - Tamaño grande 12
3.22 Piso Blanco 12
3.23 Espacio en Rack 12
3.24 Oracle 12
3.25 Microsoft SQL Server 13
3.26 Subscripciones a Bases de Datos Open Source 13
3.27 Liferay Enterprise 13
3.28 GlassFish 14
3.29 Apache Tomcat 14
3.30 Apache HTTPD 14
3.31 Servicio de correo electrónico 14
3.32 Firewall 14
3.33 IPS 14
3.34 Anti-Denegación de Servicios (DDoS) 14
3.35 Redes Privadas Virtuales – VPN 15
3.36 Gestión Unificada de Amenazas (UTM) 15
3.37 Firewall Especializado en Servicios Web (WAF) 15
3.38 Nodo de red con UTP 16
3.39 Nodo de red con Fibra Optica 16
3.40 Switch de 10G de core 16
3.41 Switch de 1G de distribución 16
3.42 Sistema de Almacenamiento de datos en RAID5 de 12TB con capacidad de crecimiento hasta 32TB 16

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	07/12/2021	Elaboración del documento	Héctor Javier Reyes Oropeza
0.2	07/12/2021	Revisión del documento	Javier Cortés López
0.3	21/12/2021	Actualización del documento	Héctor Javier Reyes Oropeza
0.4	07/03/2022	Actualización del documento	Héctor Javier Reyes Oropeza
0.5	06/05/2022	Actualización del documento	Héctor Javier Reyes Oropeza
1.0	06/05/2022	Aprobación del documento	Eduardo Oropeza Ortiz

ANEXOS
DIVISIÓN DE CONTRATOS

3.43 Solución para el cumplimiento WCAG 16
4 Proyección de crecimiento 16
5 Firmas de elaboración, revisión y aprobación 18

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 2022, 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.

Descripción	Cantidad	Unidad de medida
Servidor X86	689	Servicio
Incrementos de Módulos de 1 Procesador con 128 threads X86	44	Servicio
Incrementos de 128GB de memoria RAM X86	22	Servicio
Módulo de Seguridad en Hardware (HSM)	1	Servicio
Almacenamiento de Datos Individual	531	Servicio
Incremento de Almacenamiento de Datos Individual de 100GB	5079	Servicio
Respaldo de Datos Individual	81	Servicio
Unidad de almacenamiento de media categoría para aplicaciones de bajo desempeño	2	Servicio
Incremento en disco de estado sólido 1TB para almacenamiento bajo desempeño	1	Servicio
Incremento en disco FC solido 1TB usable para almacenamiento bajo desempeño (SATA)	16	Servicio
Unidad de respaldo de plataforma abierta	6	Servicio
Incremento de bloques de 30TB usables en arreglo RAID 5 para unidades de plataforma abierta	13	Servicio
Unidad de Almacenamiento de Datos de alto rendimiento y red SAN	1	Servicio
Incremento en discos de estado sólido 1TB para almacenamiento de alto rendimiento	98	Servicio
Unidad individual de respaldos (Portatil)	505	Servicio
Sistema Operativo Red Hat Enterprise Linux	35	Servicio
Sistema Operativo SLES	11	Servicio
Sistema Operativo Oracle Linux Server	0	Servicio
Sistema Operativo Windows Server 2008	0	Servicio
Sistema Operativo Windows 2012	0	Servicio

ANEXOS
DIVISIÓN DE CONTRATOS

Descripción	Cantidad	Unidad de medida
Servidor Virtual RISC SPARC	16	Servicio
Incremento de 1 Procesador Virtual con 128 threads RISC	11	Servicio
Incremento de 32GB de memoria Virtual RAM RISC	6	Servicio
Servidor Virtual X86 4VCPU 16 RAM	510	Servicio
Incremento Virtualizado Módulos de 1 Procesador Virtual con 8 threads X86	436	Servicio
Incremento Virtualizado 8GB de memoria RAM X86	521	Servicio
Puntos de Acceso a la Nube	1322	Servicio
Escritorio en la Nube	955	Servicio
Plataforma de Virtualizacion multi-tecnologia	2	Servicio
Punto Neutro	1	Servicio
Conectividad de Enlaces MPLS 5 Gbps redundante activo – activo	3	Servicio
Conectividad de Enlaces Lan2Lan 100 Mbps redundante activo – activo	1	Servicio
UTM para enlaces de banda ancha hasta 100 Mbps	1	Servicio
UTM para enlaces de banda ancha hasta 10 Gbps	2	Servicio
Balanceador de carga de capas L4-L7	3	Servicio
Plataforma Nodo de Extensión de Nube Privada - Tamaño grande	1	Servicio
Piso Blanco	3	Servicio
Espacio en Rack	1	Servicio
Tableau Server	0	Servicio
Tableau Desktop	0	Servicio
Bases de Datos Oracle – StandAlone	0	Servicio
Bases de Datos Oracle – RAC	0	Servicio
Microsoft SQL Server	0	Servicio
Subscripciones a Bases de Datos Open Source	1	Servicio
Java Development Kit	3	Servicio
Liferay Enterprise 7/24	8	Servicio
Liferay Enterprise 5/8	0	Servicio
Alfresco	4	Servicio
WebLogic	0	Servicio
GlassFish	8	Servicio
Apache Tomcat	1	Servicio
Apache HTTPD	97	Servicio
Servicio de correo electrónico.	92051	Servicio
Firewall	6	Servicio
IPS	2	Servicio
Anti-Denegación de Servicios (DDoS)	2	Servicio
Redes Privadas Virtuales – VPN	2	Servicio
Gestión Unificada de Amenazas (UTM)	4	Servicio
Firewall Especializado en Servicios Web (WAF)	2	Servicio
Nodo de red con UTP	629	Servicio
Nodo de red con Fibra Optica	64	Servicio
Switch de 10G de core	16	Servicio
Switch de 1G de distribución	70	Servicio
UTM para enlaces a Red Nacional para Impulso de la Banda Ancha (NIBA) de 100 Mbps	1	Servicio
Enlaces Internet 100 Mbps redundante activo – activo	4	Servicio

Descripción	Cantidad	Unidad de medida
Sistema de Almacenamiento de datos en RAID5 de 12TB con capacidad de crecimiento hasta 32TB	74	Servicio
Solución para el cumplimiento WCAG	1	Servicio

La información expresada es de carácter informativo y no representa un compromiso del Instituto respecto al comportamiento de los servicios, ya que los mismos son bajo demanda conforme a las necesidades del Instituto.

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
  - Mínimo 8 cores por procesador

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

ANEXOS
DIVISIÓN DE CONTRATOS

- 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

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

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:

ANEXOS
DIVISIÓN DE CONTRATOS

- 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 caracteristicas 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.

ANEXOS
DIVISIÓN DE CONTRATOS

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 ODI
- Sistema Operativo Oracle Linux Server
- WebLogic

3.25 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.

3.26 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.

3.27 Liferay Enterprise

ANEXOS
DIVISIÓN DE CONTRATOS

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

3.28 GlassFish

Administración de la plataforma GLASSFISH o equivalente según sean sus necesidades. Incluye las acciones necesarias para garantizar la continuidad de la operación.

3.29 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.

3.30 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.

3.31 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.

3.32 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.

3.33 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.

3.34 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.

3.35 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).

3.36 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

Los servicios de antimalware y filtrado de contenido web, deberán formar parte de los módulos del UTM integrados dentro del mismo dispositivo.

El instituto suministrará el software relacionado con el servicio del antispam.

3.37 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.

ANEXOS
DIVISIÓN DE CONTRATOS

3.38 Nodo de red con UTP

Infraestructura de conectividad física basada en conectores de cobre tipo UTP categoria 6 o superior, rematados en un rack con panel de parcheo y conectores tipo face-plate. No incluye el tendido de cableado.

3.39 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.

3.40 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

3.41 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.

3.42 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.

3.43 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	2020	2021
Servidor X86	689	

Descripción	2020	2021
Incrementos de Módulos de 1 Procesador con 128 threads X86	44	
Incrementos de 128GB de memoria RAM X86	22	
Módulo de Seguridad en Hardware (HSM)	1	
Almacenamiento de Datos Individual	531	
Incremento de Almacenamiento de Datos Individual de 100GB	5079	
Respaldo de Datos Individual	81	
Unidad de almacenamiento de media categoría para aplicaciones de bajo desempeño	2	
Incremento en disco de estado sólido 1TB para almacenamiento bajo desempeño	1	
Incremento en disco FC solido 1TB usable para almacenamiento bajo desempeño (SATA)	16	
Unidad de respaldo de plataforma abierta	6	
Incremento de bloques de 30TB usables en arreglo RAID 5 para unidades de plataforma abierta	13	
Unidad de Almacenamiento de Datos de alto rendimiento y red SAN	1	
Incremento en discos de estado sólido 1TB para almacenamiento de alto rendimiento	98	
Unidad individual de respaldos (Portatil)	505	
Sistema Operativo Red Hat Enterprise Linux	35	
Sistema Operativo SLES	11	
Sistema Operativo Oracle Linux Server	0	
Sistema Operativo Windows Server 2008	0	
Sistema Operativo Windows 2012	0	
Servidor Virtual RISC SPARC	16	
Incremento de 1 Procesador Virtual con 128 threads RISC	11	
Servidor Virtual X86 4VCPU 16 RAM	6	
Incremento Virtualizado Módulos de 1 Procesador Virtual con 8 threads X86	510	
Incremento Virtualizado 8GB de memoria RAM X86	436	
Puntos de Acceso a la Nube	521	
Escritorio en la Nube	1322	
Plataforma de Virtualizacion multi-tecnologia	955	
Punto Neutro	2	
Conectividad de Enlaces MPLS 5 Gbps redundante activo - activo	1	
Conectividad de Enlaces Lan2Lan 100 Mbps redundante activo - activo	3	
UTM para enlaces de banda ancha hasta 100 Mbps	1	
UTM para enlaces de banda ancha hasta 10 Gbps	1	
Balanceador de carga de capas L4-L7	2	
Plataforma Nodo de Extensión de Nube Privada - Tamaño grande	3	
Piso Blanco	1	
Espacio en Rack	3	
Tableau Server	1	
Tableau Desktop	0	
Bases de Datos Oracle – StandAlone	0	
Bases de Datos Oracle – RAC	0	
Microsoft SQL Server	0	

ANEXOS
DIVISIÓN DE CONTRATOS

Descripción	2020
Subscripciones a Bases de Datos Open Source	0
Liferay Enterprise 7/24	1
Liferay Enterprise 5/8	3
WebLogic	8
GlassFish	0
Apache Tomcat	4
Apache HTTPD	0
Servicio de correo electrónico.	8
Firewall	1
IPS	97
Anti-Denegación de Servicios (DDoS)	92051
Redes Privadas Virtuales - VPN	
Gestión Unificada de Amenazas (UTM)	
Filtrado de Contenido Web	
Antispam	
Antimalware	
Firewall Especializado en Servicios Web (WAF)	
Nodo de red con UTP	
Nodo de red con Fibra Optica	
Switch de 10G de core	
Switch de 1G de distribución	629
UTM para enlaces a Red Nacional para Impulso de la Banda Ancha (NIBA) de 100 Mbps	64
Enlaces Internet 100 Mbps redundante activo - activo	16
Sistema de Almacenamiento de datos en RAID5 de 12TB con capacidad de crecimiento hasta 32TB	70
Solución para el cumplimiento WCAG	

5 Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Héctor Javier Reyes Oropeza	Titular de la División de Administración de Centros de Datos.		06/05/2022

Revisó	Cargo	Firma	Fecha
Javier cortés López	Titular de la Coordinación Técnica de Operación y Administración de Centro de Datos		06/05/2022

Aprobó	Cargo	Firma	Fecha
Eduardo Oropeza Ortiz	Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional		06/05/2022

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

Apéndice 5

Especificaciones Técnicas de Seguridad de la Información

SGMP_Apéndice_5

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

ANEXOS
DIVISIÓN DE CONTRATOS

Contenido

1		Objetivo del Documento	4
2		Especificaciones para los Componentes de Infraestructura	4
	2.1	Firewall	4
	2.2	IPS	5
	2.3	Anti-denegación de Servicios (DDoS)	6
	2.4	Gestión Unificada de Amenazas (UTM)	8
	2.5	Firewall Especializado en Servicios Web (WAF)	9
	2.6	Centro de Operaciones de Seguridad (SOC)	12
3		Firmas de elaboración, revisión y aprobación	13

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	07/12/2021	Elaboración del documento	Héctor Javier Reyes Oropeza
0.2	07/12/2021	Revisión del documento	Javier Cortés López
0.3	21/12/2021	Actualización del documento	Héctor Javier Reyes Oropeza
0.4	07/03/2022	Actualización del documento	Héctor Javier Reyes Oropeza
0.5	06/05/2022	Actualización del documento	Héctor Javier Reyes Oropeza
1.0	06/05/2022	Aprobación del documento	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 Componentes de Infraestructura

2.1 Firewall

Firewall para Enlaces de Banda Ancha de hasta 100 Mbps

- Deberá contar al menos con un rendimiento de 20 Gbps, en su funcionalidad de firewall.
- Deberá tener al menos un rendimiento 5 Gbps en su funcionalidad de IPS
- Mínimo deberá contar con 8 puertos 100/1000 de cobre RJ45
- Mínimo deberá soportar 2 puertos de 10 Gbps de fibra
- Mínimo deberá contar con 32 GB de memoria Desempeño de al menos 6 mil conexiones concurrentes
- Capacidad de 150k conexiones por segundo

Los Firewall deberán cumplir con al menos las siguientes funcionalidades operativas:

- Capacidad de configurar zonas, Web, App, DB, Transversales, Monitoreo, Respaldo y Operación, entre otras.
- 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.
- Deberá ser compatible con direccionamiento IPv4 e IPv6
- Deberá contar con la capacidad de manejo de al menos 1024 Vlans.
- 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 diversas cipher suites en Secure Sockets Layer (SSL) y Transport Layer Security (TLS).
- Deberá soportar la integración de certificados.
- Deberá soportar la conexión de dispositivos móviles a través de un cliente de acceso remoto especifico. Dicho cliente debe soportar al menos las siguientes plataformas: MAC OS X desde v10.12, iOS desde v5, Android desde v4.2, Windows desde v10.

- Administración del sistema vía Web (HTTPS), por la línea de comando (SSH), soportar SNMPv3 y a través de una consola central de administración.
- Deberá contar con administración de políticas de al menos 500 limitado por capacidad máxima del equipo.
- Deberá contar con la capacidad de guardar histórico de cambios sobre las políticas.
- Deberá contar con doble fuente de poder que pueda ser sustituida en caliente sin afectar al dispositivo y al servicio que presta
- 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.

2.2 IPS

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

- Soporte de al menos: 20Gbps de inspección.
- Latencia máxima de 0.5 milisegundos.
- Soporte de 4 Interfaces de 10G
- Soporte Interface RJ45 para administración
- Deberá operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP.
- Capacidad de detección en línea sin bloquear tráfico (Modo transparente). El sistema sólo alertará que eventos serian bloqueados.

AUTOS
DIVISIÓN DE CONTRATOS

- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, 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

2.3 Anti-denegación de Servicios (DDoS)

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

- La solución deberá ofrecer el licenciamiento o suscripción necesario para operar en cualquiera de los ambientes sin necesidad de que la institución requiera adquirir hardware/software adicional y de manera ilimitada
- La solución deberá soportar al menos 250 Mbps.

- La solución deberá proteger al menos 2 redes IPv4 clase C con un esquema de redundancia contra ataques DDoS
- La solución deberá proporcionar los mecanismos necesarios para la mitigación de todos los tipos de ataques DDoS, ya sean basados en la Red (Capa 3, 4) o ataques de nivel aplicativo (Capa 7). Teniendo en cuenta la siguiente lista:
    - TCP SYN+ACK
    - TCP FIN
    - TCP RESET
    - TCP ACK
    - TCP ACK+PSH
    - TCP Fragment
    - UDP
    - ICMP
    - IGMP
    - HTTP Flood
    - Brute Force
    - Connection Flood
    - Slowloris
    - Spoofing
    - DNS Flood
    - Mixed SYN+UDP or ICMP+UDP Flood
    - TCP SYN+ACK
    - Ping Of Death
    - Smurf
    - Reflected ICMP and UDP
    - Teardrop
    - Zero-day DDoS attacks
- Protección contra ataques de fuerza bruta y DDoS
- Servicio de Mitigación de ataques DDoS a los aplicativos Web
- Servicio de Mitigación de ataques DDoS al servicio DNS
- Para la mitigación de ataques DDoS al servicio DNS, la plataforma de nube deberá tomar el rol de NS (NameServer), designado a través del sistema DNS global, para que sea la primera instancia que reciba peticiones de DNS provenientes de Internet y destinadas a la infraestructura; y las reenvíe después de la inspección de seguridad.
- Deberá de tener la capacidad de definir las solicitudes de DNS válidos, en cuanto a tipo y dominio, que habrá de dejar pasar a los servidores DNS reales, bloqueando el resto de las peticiones
- Servicio de Mitigación de ataques DDoS para la Suite TCP/IP de la red pública del instituto
- Herramientas de monitoreo en tiempo real de conexiones, ancho de banda y ataques.
- Servicio de protección para API
- Servicio de prevención contra robo de cuentas de administrador
- Monitoreo y control de vulnerabilidades en las aplicaciones web críticas
- Protección avanzada contra tráfico malicioso automatizado (BOTs)
- Protección contra el uso de recursos de terceros com JavaScript en las aplicaciones Web
-
- La solución como servicio deberá garantizar un SLA del 99.999%

DIVISIÓN DE CONTRATOS

- El proveedor deberá contar con una capacidad de red global de al menos 6.5 Tbps de contención

2.4 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: 3Gbps de inspección.
  - Latencia máxima de 0.5 milisegundos.
  - Podrá operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP.
  - Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, 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 hosts de la red y crear una alarma cuando cierto umbral sea rebasado.

- Funcionalidad Filtrado de Contenido Web
  - 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.
  - 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 diversas cipher suites en Secure Sockets Layer (SSL) y Transport Layer Security (TLS).
  - Deberá soportar la integración de certificados.

2.5 Firewall Especializado en Servicios Web (WAF)

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

- Se requiere una solución que sea capaz de operar en ambientes físicos y/o virtuales en las instalaciones de la institución (On-Premise), servicios de nube como Amazon Web Services, Microsoft Azure y compatible con Google Cloud además de ofrecer la opción de protección de aplicaciones sin necesidad de instalación de hardware y/o software, es decir, como servicio.
- La solución deberá ofrecer el licenciamiento necesario para operar en cualquiera de los ambientes descritos sin necesidad de que la institución requiera adquirir hardware/software adicional y de manera ilimitada.

ANEXOS
DIVISIÓN DE CONTRATOS

- En caso de que la institución requiera desplegar Appliances virtuales adicionales en nube privada y/o pública, se podrá realizar sin ningún costo adicional y de manera ilimitada.
- La solución deberá soportar cualquier aplicación web, sin importar la plataforma, tamaño del sitio, lenguaje o escenario de implementación.
- La solución deberá soportar las 80 aplicaciones Web de la institución, así como un consumo promedio mensual de 300 Mbps.
- La solución deberá ofrecer los siguientes servicios en una única plataforma integrada
- El modelo positivo de seguridad deberá definir lo que está permitido y bloquear todo lo demás. Deberá incluir direcciones URL, directorios, cookies, campos, parámetros (identificando además el formato y tipo de estos), métodos HTTP.
- Para facilitar la configuración del modelo positivo de seguridad, el dispositivo deberá aprender automáticamente la estructura y los elementos de la aplicación de manera constante y sin intervención humana.
- La configuración aprendida deberá ser accesible y modificable para el administrador de la solución.
- La solución deberá correlacionar múltiples eventos de seguridad para distinguir tráfico deseado del tráfico inadecuado.
- 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 Web. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:
    - Estado de autenticación de la sesión web
    - Por el URL de autenticación y el resultado del intento de autenticación
    - Por URL, a través del prefijo, ruta o host.
    - Por la existencia o contenido de cualquier header HTTP
    - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier personalización por expresiones regulares), ya sea en las operaciones http-request o http-response por parte del servidor Web
    - Host o dominio accedido
    - Por el protocolo usado, HTTP o HTTPS
    - Dirección IP origen
    - Por la existencia o contenido de cookies o el identificador de sesión
    - Fecha y hora del evento
    - Por usuario firmado en el aplicativo web
    - User-Agent
    - Referer-URL
    - Tiempo de respuesta o tamaño de la respuesta HTTP
- La solución deberá entregar un análisis detallado de las amenazas, incluyendo:
    - Dirección IP
    - Locación geográfica
    - Información relevante de la sesión
- La solución deberá cubrir todas las vulnerabilidades expresadas en el OWASP Top Ten más reciente.
- El servicio deberá ser capaz de mitigar el riesgo por vulnerabilidades no parchadas tales como:
    - Command Injection
    - Clickjacking
    - Cross-Site Scripting (XSS)
    - Cross-Site Request Forgery (CSRF/XSRF)
    - Violaciones de acceso a la base de datos
    - Inyección HTML

- Cookies Inseguras
- Inyección JSON
- Malformed Content-Types
- Path Traversal

- Deberá ser reconocido como al menos "Leaders" en el The Forrester Wave: Web Application Firewalls, Q4 2017
- Deberá aparecer y ser consiste en la aparición en el cuadrante mágico de Gartner de al menos los últimos 6 años
- Red de entrega de contenido (CDN por sus siglas en inglés) con conmutación en caso de falla y redundancia
  - Almacenamiento en caché para mejoramiento de la experiencia de uso
  - Optimización de contenido entregado por la aplicación Web
  - Reglas de personalización de caché
- Balanceo global y conmutación en caso de fallas (failover) de cargas global
- Funcionales de la plataforma on-premise o virtual
- La solución deberá brindar la protección a los aplicativos cuya comunicación o publicación se limite a la red interna del instituto
- La solución deberá ser capaz de desplegarse en ambientes físico o virtual dentro de la infraestructura de la organización (On-Premise):
  - Los diferentes componentes de seguridad de los aplicativos distribuidos en red deberán de administrarse a través de una consola centralizada.
  - La solución propuesta deberá estar soportada en arquitectura de Alta Disponibilidad (HA)
  - La solución propuesta deberá tener un rendimiento de 10 Gbps.
  - La solución deberá soportar ser desplegada o implementada en línea como un puente o bridge transparente (capa 2 del Modelo OSI) las interfaces no requerirán de una dirección IP, como un proxy transparente o un proxy inverso (según se requiera), o como un analizador no en línea a través de puertos Mirror o SPAN.
  - Los Appliances físicos deberán soportar el modo bypass/fail-open/fail-closed configurable tanto para fallas de hardware como software.
  - En el modo monitoreo el administrador podrá visualizar alertas, ataques, errores de servidor y otra actividad no autorizada.
  - En el modo de cumplimiento de políticas, la solución deberá bloquear ataques proactivamente.
  - Respecto de algún ataque o alguna otra actividad no autorizada, la solución deberá ser capaz de tomar las acciones adecuadas. Las acciones deberán incluir la habilidad para terminar las solicitudes y respuestas, bloquear la sesión TCP, bloquear el usuario de la aplicación, o bloquear la dirección IP.
  - Respecto de ataques particularmente destructivos, la solución deberá ser capaz de bloquear la dirección IP por un periodo de tiempo configurable.
  - En modo analizador de paquetes, la solución deberá ser capaz de enviar un paquete TCP-RST a ambos extremos de la conexión. Alternativamente, si así se configura, la solución podrá reportar el comportamiento anómalo, pero no tomar acción alguna.
  - La solución podrá ser desplegada dentro de ambientes virtuales VMWare y/o Microsoft Hyper-V como dispositivo virtual.
  - Los Appliances físicos deberán soportar el volumen de tráfico y deberá tener una latencia menor a 5 ms, para no impactar el desempeño de las aplicaciones.
  - Para el dispositivo físico la solución deberá soportar las siguientes opciones de conectividad física por dispositivo:

ANEXOS
DIVISIÓN DE CONTRATOS

- 4 interfaces de 10 GB en Fibra Óptica tipo SX
- Para los dispositivos físicos las interfaces de conectividad a la red deberán de ser modulares para tener la posibilidad de hacer cambios de medio como por ejemplo Cobre UTP a Fibra Óptica y viceversa, sin necesidad de cambiar el dispositivo.
- La solución deberá proporcionar una vista unificada con el objetivo de facilitar el monitoreo todos los eventos de seguridad relacionadas con el uso de aplicaciones Web.

2.6 Centro de Operaciones de Seguridad (SOC)

Perfil	Certificaciones a demostrar	Función	Número de recursos
Administrador del Centro de Operaciones de Seguridad (SOC 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 las aplicaciones y la infraestructura, así como prever, detectar, analizar, contener, erradicar, documentar incidente de seguridad.	Al menos 1
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	Al menos 3, o los necesarios

Perfil	Certificaciones a demostrar	Función	Número de recursos
		los servicios, así como del registro y seguimiento de solicitudes de ventanas de mantenimiento, reportes de fallas y requerimientos.	para garantizar el servicio 7x24x365 durante la vigencia del contrato

3 Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Héctor Javier Reyes Oropeza	Titular de la División de Administración de Centros de Datos.		06/05/2022

Revisó	Cargo	Firma	Fecha
Javier cortés López	Titular de la Coordinación Técnica de Operación y Administración de Centro de Datos		06/05/2022

Aprobó	Cargo	Firma	Fecha
Eduardo Oropeza Ortiz	Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional		06/05/2022

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

Apéndice 6

Métricas de Niveles de Servicio

SGMP_Apéndice_6

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

ANEXOS
DIVISIÓN DE CONTRATOS

Contenido

1 Objetivo del Documento 4
2 Métrica de Disponibilidad 4
3 Penalizaciones y Deducciones al Pago 6
3.1 Penas Convencionales 6
3.2 Deducciones por Incumplimiento de Niveles de Servicio (SLAs) 8
3.2.1 Deductivas sobre SLAs aplicables a todos los servicios del Anexo Técnico 8
4 Firmas de elaboración, revisión y aprobación 8

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	07/12/2021	Elaboración del documento	Héctor Javier Reyes Oropeza
0.2	07/12/2021	Revisión del documento	Javier Cortés López
0.3	07/03/2022	Actualización del documento	Héctor Javier Reyes Oropeza
0.3	06/05/2022	Actualización del documento	Héctor Javier Reyes Oropeza
1.0	06/05/2022	Aprobación del documento	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.
  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.

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:

$$\text{Disponibilidad}_i = 100 * (TRO_i / (TTM_i - TPFO_i))$$

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 número 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 las 24 horas los 7 días de la semana
- 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:

Ubicacines	Componentes de Infraestructura mensual	
Centro de Datos Primario (Ambientes Productivos y no Productivos)	Disponibilidad Directa e Indirecta *	99.982%
Extensión de Nube Privada (ATOM)	Disponibilidad Directa e Indirecta ** *	99.982%
Servicios desplegados en Instalaciones designadas por el Instituto	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	-

DIVISIÓN DE CONTRATOS

Ubicacines	Componentes de Infraestructura mensual
	el presente anexo técnico) parcial o total.

** Periodo mensual en porcentaje de disponibilidad*
*** El Instituto procederá a aplicar la métrica de penalización correspondiente si el licitante incumple con la fecha compromiso registrada en la herramienta conforme al numeral 4.2.1.1.6. Mesa de servicio del Anexo Técnico.*

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.

Deductiva a aplicar al licitante ganador = (n * Monto del servicio correspondiente entregado por el proveedor o prestador de servicio), siempre y cuando sean imputables al licitante adjudicado..

3 Penalizaciones y Deducciones al Pago

3.1 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.

El criterio para considerar concluida la migración desde el Centro de Datos actual hacia el Centro de Datos ofertado, será en el momento en que se encuentren los servicios descritos anteriormente activos y operando en la infraestructura propuesta por el Licitante, e interactuando con el ecosistema tecnológico institucional, esto es; con los ambientes operativos digitales productivos y no productivos instalados en los diferentes centros de datos IMSS y del Gobierno Federal así como organismos con los que interactúa el Instituto tales como SAT, RENAPO, INFONAVIT, BANCO DE MÉXICO, PROCESAR, CONSAR, BANCOS Y AFORES, entre otros, validados de conformidad por el personal

que el Instituto designe (áreas de telecomunicaciones y seguridad informática, infraestructura tecnológica, desarrollo, monitoreo así como el personal de las direcciones normativas que hacen uso de los servicios en los casos que aplique).
Para el caso del incumplimiento del programa de trabajo ofertado para la implementación de los servicios por el Licitante en su propuesta, la penalización será del 2.5% (dos punto cinco por ciento) por cada día natural de atraso del costo mensual unitario de los servicios no entregados.

Durante la vida del contrato, la pena convencional por atraso en la entrega de la infraestructura adicional necesaria para dar continuidad a los servicios Institucionales será del 2.5% (dos punto cinco por ciento) por cada día natural de atraso del servicio en la entrega del costo mensual del servicio ofertado.

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, instalaciones designadas por el Instituto, pruebas en ambientes no productivos, entre otros), respecto al costo mensual del servicio ofertado al cual corresponda el incumplimiento, sobre las fechas establecidas de entrega, siempre y cuando sean imputables al licitante adjudicado.

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 de 0.5% (cero punto cinco) del Servicio de Soporte de Servicio de Continuidad a la Operación y Soporte de la Nube IMSS, ID 183 del formato de propuesta económica, por cada día natural de atraso

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

ANEXOS
DIVISIÓN DE CONTRATOS

3.2 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.

3.2.1 Deductivas sobre SLAs aplicables a todos los servicios del Anexo Técnico

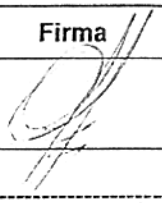
Modalidad	BCF o BCC mensual	
Centro de Datos Primario (Ambientes Productivos y no Productivos)	Disponibilidad Directa e Indirecta *	99.982%
	Deducción**por cada punto porcentual (1%)o fracción fuera del nivel de servicio	10%
Extensión de Nube Privada (ATOM)	Disponibilidad Directa e Indirecta *	99.982%
	Deducción**por cada punto porcentual (1%) o fracción fuera del nivel de servicio	10%
Servicios desplegados en Instalaciones designadas por el Instituto	Disponibilidad Directa e Indirecta *	99.982%
	Deducción**por cada punto porcentual (1%) o fracción fuera del nivel de servicio	5%
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

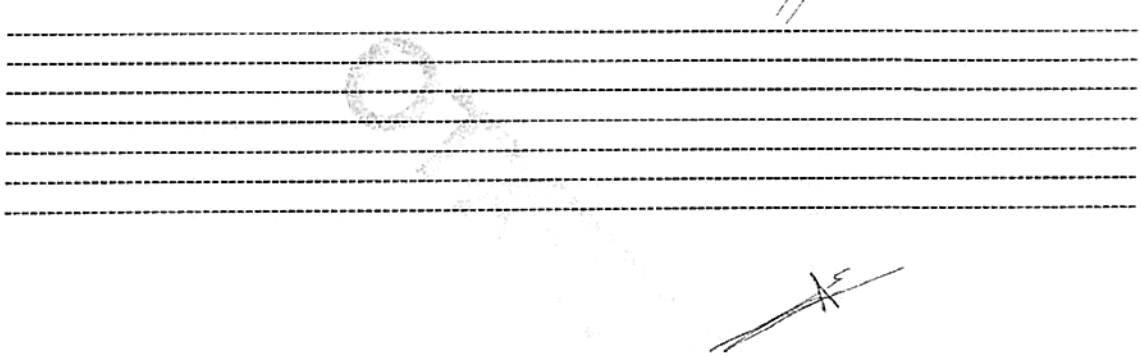
* Periodo mensual en porcentaje de disponibilidad
**Deducciones por incumplimiento sobre el precio unitario mensual del BCF o BCC afectado Por cada punto porcentual o fracción de disponibilidad.fuera del nivel de servicio solicitado

4 Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Héctor Javier Reyes Oropeza	Titular de la División de Administración de Centros de Datos.		06/05/2022

Revisó	Cargo	Firma	Fecha
Javier cortés López	Titular de la Coordinación Técnica de Operación y Administración de Centro de Datos		06/05/2022

Aprobó	Cargo	Firma	Fecha
Eduardo Oropeza Ortiz	Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional		06/05/2022



ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

Apéndice 7

Glosario Nube IMSS

SGMP_Apéndice_7

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

ANEXOS
DIVISIÓN DE CONTRATOS

Contenido

1	Objetivo del Documento	4
2	Glosario	4
3	Tabla de Acrónimos	8
4	Firmas de elaboración, revisión y aprobación	10

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	07/12/2021	Elaboración del documento	Héctor Javier Reyes Oropeza
0.2	07/12/2021	Revisión del documento	Javier Cortés López
0.3	07/03/2022	Actualización del documento	Héctor Javier Reyes Oropeza
0.4	06/05/2022	Actualización del documento	Héctor Javier Reyes Oropeza
1.0	06/05/2022	Aprobación del documento	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. Modelo de entrega de servicios tecnológicos cuya implementación asegura un grado mayor de continuidad operacional durante un periodo de medición determinado.

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.

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 medios electrónicos; "enrutar" los mensajes en función de quien los emite explicitando el motivo; gestionar alarmas y acciones que permitan brindar servicios 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.

CI/CD. Prácticas combinadas de integración continua y entrega continua (también conocida como despliegue continuo) que promueven la automatización de parte del proceso de desarrollo de software.

Componente Tecnológico: Se refiere a cualquier componente de un servicio, elemento de infraestructura u otro elemento que requiere ser administrado para asegurar la entrega correcta de los servicios.

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.

Contenedores. Es una tecnología que propone el empaquetamiento de una aplicación en conjunto con sus componentes y dependencias asociadas a sus tiempos de ejecución.

Despliegue. Instalación o implantación de un Activo o Servicio de TI dentro de un determinado entorno operativo.

DevOps. Es una práctica de ingeniería de software que tiene como objetivo unificar el desarrollo de software (Dev) y la operación del software (Ops). Su principal característica es promover la automatización y el monitoreo en todos los pasos de la construcción del software, desde la integración, las pruebas, la liberación hasta la implementación y la administración de la infraestructura.

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.

Elemento de Configuración (CI). Se refiere a cualquier componente de un servicio, elemento de infraestructura u otro elemento que requiere ser administrado para asegurar la entrega correcta de los servicios.

ANEXOS
DIVISIÓN DE CONTRATOS

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.

Evaluación de madurez. Es un modelo descriptivo que mide los atributos esenciales que caracterizan una organización en un nivel particular de la adopción en la gestión de cierta área de conocimiento (como puede ser la Arquitectura Empresarial o los nuevos esquemas de desarrollo como DevOps). También es un modelo normativo en el que las prácticas principales caracterizan los tipos ideales de ambiente que deberían esperarse en una organización que esté implementando gestión de dichas áreas de conocimiento.

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.

Kubernetes. Es una plataforma de contenedores portable y extensible de código abierto que se utiliza para administrar cargas de trabajo y servicios. Esta plataforma facilita la automatización y la configuración declarativa.

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.

Modelo de Gobierno. Es la disciplina que propone llevar a cabo la gestión de los diferentes componentes y servicios de TI, basada en la definición de procesos y roles alineados al cumplimiento de los objetivos de una organización.

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.)

ANEXOS
DIVISIÓN DE CONTRATOS

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.

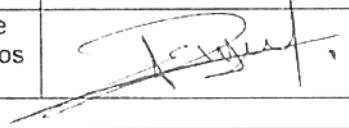
3 Tabla de Acrónimos

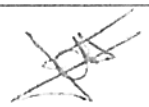
Acrónimo	Descripción
ACL	Lista de Control de Acceso (del inglés, Access Control List)
API	Interfaz de programación de aplicaciones (del inglés, *Application Programming Interface*)
BB	Bloque de Construcción (del inglés, Building Block)
BCC	Bloques de Construcción Comunes
BCF	Bloques de Construcción Fundamentales o componente de infraestructura
CAB	Consejo Consultor de Cambios (del inglés, Change Advisory Board)
CAT	Centro de Arquitectura Tecnológica
CDP	Centro de Datos Primario
CI	Elemento de configuración (del Inglés *Configuration Item*)
CI/CD	Integración Continua / Desarrollo Continuo
CCTV	Circuito Cerrado de Televisión
CMDB	Base de Datos de Elementos de Configuración (del inglés, Configuration Management Database)
DIDT	Dirección de Innovación y Desarrollo Tecnológico
DRP	Plan de Recuperación en caso de Desastres (del Inglés, Disaster Recovery Plan)
ECAB	Consejo Consultor de Cambios Emergentes (del inglés, Emergency Change Advisory Board)
EDN	Estrategia Digital Nacional
EN	Escritorios en la Nube
ENH	Extensión de Nube Híbrida
ENP	Extensión de Nube Privada
GB	Gigabytes (métrica para cuantificar una capacidad de almacenamiento de información digital)
Gbps	Gigabits por Segundo (métrica para cuantificar la velocidad de transmisión de información entre dos sistemas digitales)
HSM	Módulo de Seguridad en Hardware (del Inglés *Hardware Security Module*)
IaaS	Infraestructura como un Servicio (del inglés, Infrastructure as a Service)
IMSS	Instituto Mexicano del Seguro Social

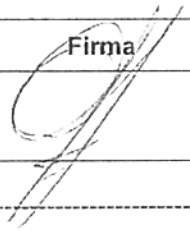
Término	Descripción
ISO	Organización Internacional para la Estandarización (del inglés, International Organization for Standardization)
ISP	Proveedor de Servicios de Internet (del inglés, Internet Service Provider)
ITIL	Biblioteca de Infraestructura de Tecnologías de Información (del inglés, Information Technology Infrastructure Library)
LAN	Red de Área Local (del inglés, Local Area Network)
LED	Diodo Emisor de Luz (del inglés, Light Emisor Diode)
MAAGTICSI	Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información
MB	Megabytes
Mbps	Megabits por Segundo
MOSNI	Marco Operativo de los Servicios de Nube IMSS
MPLS	Conmutación Multi-Protocolo mediante Etiquetas (del inglés, Multiprotocol Label Switching)
MTR	Marco Tecnológico de Referencia
NIST	National Institute of Standards and Technology
OLA	Acuerdos de Nivel de Operación (del inglés, Operational Level Agreement)
PaaS	Plataforma como un Servicio (del inglés, Platform as a Service)
PAN	Puntos de Acceso a la Nube
PDA	Asistente Digital Personal (del inglés, Personal Digital Assistant)
PEP	Portafolio Estratégico de Proyectos
PND	Plan Nacional de Desarrollo
RFC	Solicitud de Cambio (del inglés, Request for Change)
RFI	Solicitud de información (del inglés, Request for information)
RPO	Punto Objetivo de Recuperación, por sus siglas en inglés
RTO	Tiempo Objetivo de Recuperación, por sus siglas en inglés
SaaS	Software como un Servicio (del inglés, Software as a Service)
SCO	Servicio de Continuidad Operativa
SDI	Servicios desplegados en Instalaciones designadas por el Instituto
SLA	Acuerdos de niveles de servicios (del inglés, Service Level Agreement)
TB	Terabytes
TIC	Tecnologías de Información y Comunicaciones
UANP	Usuario de Acceso a la Nube Privada
UGD	Unidad de Gobierno Digital
VRF	Virtual Routing and Forwarding por sus siglas en inglés

ANEXOS
DIVISIÓN DE CONTRATOS

4 Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Héctor Javier Reyes Oropeza	Titular de la División de Administración de Centros de Datos.		06/05/2022

Revisó	Cargo	Firma	Fecha
Javier cortés López	Titular de la Coordinación Técnica de Operación Administración de Centro de Datos		06/05/2022

Aprobó	Cargo	Firma	Fecha
Eduardo Oropeza Ortiz	Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional		06/05/2022

Términos y Condiciones

SGMP_TerminosCondiciones

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de la Nube IMSS 2022

ANEXOS
DIVISIÓN DE CONTRATOS

Contenido

1. Objetivo del documento 4
2. Alcance del Servicio 4
3. Requerimientos Técnicos 5
4. Plazo de los servicios 6
5. Perfil del proveedor 6
6. Cumplimiento de obligaciones contractuales 9
7. Cláusulas y Cumplimientos 9
8. Administradores del contrato 12
9. Derechos de Autor 12
10. Confidencialidad 12
11. Conformación de la Propuesta 13
12. Garantías 16
13. Niveles de Servicio 17
14. Penas convencionales y Deductivas 17
15. Acuerdos de Niveles Operacionales 17
16. Ubicaciones para la prestación del servicio 18
17. Consideraciones para la finalización del contrato 18
18. Pago de los Servicios 18
19. Mecanismos de control para la administración del contrato 21
20. Criterio de evaluación 23
21. Licencias, permisos, registros, certificados o autorizaciones que debe cumplir o aplicarse al bien o servicio a contratar. 23
22. Folletos, catálogos, fotografías, manuales entre otros, en caso de que se requieran para comprobar las especificaciones técnicas requeridas. 23
23. Visitas a las instalaciones institucionales, donde se suministrarán o colocarán los bienes o donde se prestarán los servicios, en su caso. 23
24. En su caso, mecanismos requeridos al proveedor para responder por defectos o vicios ocultos de los bienes o de la calidad de los servicios. 23
25. Responsabilidad 23
26. Responsabilidad Laboral 24
27. Firmas de elaboración, revisión y aprobación 24

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	07/12/2021	Elaboración del documento	Héctor Javier Reyes Oropeza
0.2	07/12/2021	Revisión del documento	Javier Cortés López
0.3	21/12/2021	Actualización del documento	Héctor Javier Reyes Oropeza
0.4	07/03/2022	Actualización del documento	Héctor Javier Reyes Oropeza
0.5	18/04/2022	Actualización del documento	Héctor Javier Reyes Oropeza
0.6	06/05/2022	Actualización del documento	Héctor Javier Reyes Oropeza
1.0	18/04/2022	Aprobación del documento	Eduardo Oropeza Ortiz

DIVISIÓN DE CONTRATOS

1. Objetivo del documento

Definir al **LICITANTE** los términos y condiciones del **Servicio de Continuidad de la Nube IMSS 2022**.

2. Alcance del Servicio

El **LICITANTE** deberá brindar continuidad operativa, soporte, gestión de la operación de los servicios, aplicaciones y componentes que permiten al Instituto disponer de las capacidades de infraestructura de procesamiento, almacenamiento, respaldo, comunicaciones, seguridad, plataformas tecnológicas y software, que hoy en día se encuentran desplegadas en las siguientes ubicaciones:

- CDP - Centro de Datos Primario (Ambientes Productivos y no Productivos)
- ENP - Extensión de Nube Privada (ATOM)
- SDI - Servicios desplegados en Instalaciones designadas por el Instituto

Centro de Datos Primario

El Instituto habilitará los mecanismos idóneos para garantizar la continuidad operativa, soporte y gestión de la operación de la infraestructura actual del centro de datos primario (aplicaciones, servicios, infraestructura de procesamiento, almacenamiento y respaldo, infraestructura de seguridad y telecomunicaciones), en tanto se lleva a cabo la migración del Centro de Datos Actual a la infraestructura del Centro de Datos ofertado por el **LICITANTE** adjudicado, garantizando la operación de los aplicativos, servicios e infraestructura, de acuerdo a los niveles de servicio establecidos 99.982% de disponibilidad.

Extensión de Nube Privada (ATOM)

El **LICITANTE** adjudicado una vez concluida la migración debe brindar continuidad del servicio, soporte y gestión de la operación 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.

Servicios desplegados en instalaciones designadas por el Instituto

El **LICITANTE** adjudicado una vez concluida la migración debe brindar continuidad del servicio, soporte y gestión de la operación de infraestructura, por ejemplo, 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.

Ambientes no productivos en el Centro de Datos

El **LICITANTE** adjudicado una vez concluida la migración debe brindar continuidad operativa, soporte y gestión de la operación de la infraestructura actual del centro de datos que contenga ambientes no productivos (aplicaciones no productivas, servicios, infraestructura de procesamiento,

almacenamiento y respaldo, infraestructura de seguridad y telecomunicaciones), así como su migración del Centro de Datos Actual a la infraestructura del Centro de Datos ofertado por el **LICITANTE**, garantizando la operación de los aplicativos, servicios e infraestructura, de acuerdo a los niveles de servicio establecidos 99.982% de disponibilidad.

Comunicaciones

El **LICITANTE** adjudicado una vez concluida la migración debe brindar continuidad operativa, soporte y gestión de la operación de la solución de telecomunicaciones, incluyendo acciones para habilitación de infraestructura de conectividad en red con la funcionalidad de "Punto Neutro" durante el primer semestre del servicio, la cual deberá tener la capacidad de concentrar los enlaces de telecomunicaciones de las diferentes redes de telecomunicaciones del IMSS y proporcionadas por diversos prestadores de servicio, así como los enlaces de telecomunicaciones de los principales organismos públicos y privados con los que el Instituto interactúa. El servicio debe incluir la conectividad actual de 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.

El **LICITANTE** adjudicado una vez concluida la migración debe brindar la continuidad a los servicios, aplicativos, servicios digitales y de información, así como su interconexión con los centros de datos propios del Instituto o del Gobierno Federal y entidades externas (tales como: SAT, RENAPO, Procesar, Banco de México, INFONAVIT, Bancos, Instituto Nacional Electoral, Afores, CONSAR, entre otros) que permitan el intercambio de información, conforme a los estándares de telecomunicaciones y seguridad definidos por el Instituto.

3. Requerimientos Técnicos

El **LICITANTE** adjudicado una vez concluida la migración debe brindar continuidad operativa, soporte y gestión de la operación de la solución de infraestructura de procesamiento, almacenamiento, respaldos, telecomunicaciones y seguridad, así como a las aplicaciones, componentes y servicios digitales del Instituto en sus diversos esquemas desplegados, tales como: Centro de Datos Actual, Nodo de Extensión de Nube y Ubicaciones designadas por el Instituto, así como las que el Instituto designe durante la vigencia del Servicio.

Los servicios requeridos por el Instituto y que el **LICITANTE** deberá proveer durante la vigencia del servicio son los siguientes:

- Servicio de Continuidad Operativa y Soporte
- Servicio de Continuidad y Soporte de Telecomunicaciones
- Servicio de Continuidad y Soporte de Seguridad

Para cada servicio antes mencionado, se requiere que el **LICITANTE** integre como parte de la ejecución del servicio, los esquemas de Gestión de la Operación y Soporte, así como el Aprovisionamiento de infraestructura bajo demanda relativa a procesamiento, almacenamiento, respaldos, telecomunicaciones y seguridad.

La siguiente tabla muestra de manera enunciativa más no limitativa el esquema de organización de cada servicio:

ANEXOS
DIVISIÓN DE CONTRATOS

Nombre del Servicio	Continuidad y Soporte bajo demanda	Aprovisionamiento de Infraestructura bajo demanda
Servicio de Continuidad Operativa y Soporte a la Operación	Servicios bajo demanda de continuidad operativa, gestión de la operación y soporte de la infraestructura de procesamiento, almacenamiento y respaldos, así como a las aplicaciones, componentes y servicios digitales del Instituto en cualquiera de sus capas (web, aplicativa, base de datos, balanceo etc.)	Aprovisionamiento de infraestructura de procesamiento, almacenamiento y respaldos, bajo demanda.
Servicio de Continuidad y Soporte de Telecomunicaciones	Servicios bajo demanda de continuidad operativa, gestión de la operación y soporte referente a componentes e infraestructura de telecomunicaciones, así como la interconexión entre los diferentes ecosistemas Institucionales, así como con otras entidades públicas y privadas.	Aprovisionamiento de infraestructura de telecomunicaciones, bajo demanda.
Servicio de Continuidad y Soporte de Seguridad	Servicios bajo demanda de continuidad operativa, gestión de la operación y soporte referente a componentes e infraestructura de seguridad física y lógica.	Aprovisionamiento de infraestructura de seguridad, bajo demanda.

El **LICITANTE** debe proveer el soporte técnico en caso de falla en un esquema de 7 dias 24 horas durante la vigencia del servicio.

A continuación, se describe el objetivo de cada servicio requerido por el Instituto y que el **LICITANTE** adjudicado deberá brindar como parte de los servicios.

4. Plazo de los servicios

La vigencia del contrato y el plazo para la para la prestación del servicio será a partir del día siguiente de la fecha de adjudicación y hasta el 31 de diciembre de 2022

La definición de la programación, implementación y desarrollo de los servicios se establece en el correspondiente Anexo Técnico.

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 de al menos 5 años para brindar los servicios objeto del presente anexo técnico, apéndices, así como términos y condiciones, para lo cual deberá de presentar copia de contratos, pedidos o convenios formalizados con el sector público o privado cuyo objeto esté relacionado con los servicios de la presente licitación.

El **LICITANTE** deberá contar con especialidad comprobable de al menos 5 contratos formalizados cuyo objeto esté relacionado con la prestación de servicios similares al de la presente licitación.

El **LICITANTE** deberá cumplir con las siguientes certificaciones de Centros de Datos así como, de Gestión del Servicio que se listan de manera enunciativa más no limitativa en la siguiente tabla:

Componente o Servicio	Descripción	Especificación	Tipo
Certificación de Centros de Datos	Certificación de Disponibilidad del Centro de Datos Ofertado	TIER III o ICREA IV equivalente o superior	Funcional
Gestion de Servicios de Tecnologias de la Información y Comunicaciones.	Certificación de gestion de procesos de Tecnologias de la Informacion y Comunicaciones.	ITIL V3 equivalente o superior	Funcional
Sistemas de Gestion del Servicio	Calidad en la Gestion de Servicios de TIC	ISO/IEC 20000-1 equivalente o superior	Funcional
Gestión de Seguridad de la Información	Implementación, Mantenimiento y Gestion de Sistemas de Gestión de Seguridad de la Información	ISO 27001 equivalente o superior	Funcional

Certificaciones enunciativas más no limitativas, o en su caso, similares en funcionalidad o tema en:

- **ISO/IEC 27001**
- **ISO/IEC 20000**
- **ITIL Expert Certificate**
- **ITIL Foundation Certificate in IT Service Management**
- **ITIL intermediate in Operational support and analysis**
- **ITIL intermediate in Service Offering AND Agreements**
- **ITIL intermediate un Release, control and validación**

El Administrador de proyectos deberá contar con las siguientes certificaciones:

- **Project Management Institute (PMI)**
- **ITIL Foundation Certificate in IT Service Management version 4**
- **Scrum Certified Master**

El **LICITANTE** deberá contar con el personal certificado en Metodologías de Administración de Proyectos para la dirección del proyecto.

ANEXOS
DIVISIÓN DE CONTRATOS

El **LICITANTE** deberá contar con el personal certificado o con experiencia comprobable en productos, software y componentes descritos en el presente anexo técnico por lo que deberá adjuntar a su propuesta las siguientes certificaciones:

- **CCNA - Cisco Certified Network Associate**
- **CCNA - Cisco Certified Network Associate Routing and Switching**
- **CCNP - Cisco Certified Network Professional**
- **Cisco Certified Specialist - Data Center Core**
- **CISM - Certified Information Security Manager**
- **CISSP Certified Information Systems Security Professional**
- **MCITP Enterprise Administrator on Windows Server 2008**
- **MCTS Microsoft Exchange Server 2007 Configuration**
- **Scrum Master Certified Credential**
- **Exchange Server 2007 Configuration**
- **Windows Server 2008 Active Directory, Configuring**
- **Windows Server 2008 Applications Infrastructure, Configuring**
- **Windows Server 2008 Network Infrastructure, Configuring**
- **Windows Server 2008, Enterprise Administrator**
- **Microsoft SQL Server 2008, Implementation and Maintenance**
- **Oracle Certified Associate - Oracle WebLogic Server 11g System Administrator**
- **Oracle Database 11g: Administrator Certified Associate**
- **Oracle Database 11g: Administrator Certified Professional**
- **Oracle Database 12c Certified Implementation Specialist**
- **Oracle WebLogic Server 12c Administrator**
- **Oracle VM 3.0 for x86 Certified Implementation Specialist**
- **VMware Certified Professional Data Center Virtualization 2019 o superior**
- **Querying Microsoft SQL Server 2012/2014 o superior**
- **Administering Microsoft SQL Server 2012/2014 Databases**
- **Implementing a Data Warehouse with Microsoft SQL Server 2012/2014**
- **Microsoft Certified Solutions Associate SQL Server 2012/2014**
- **Red Hat Certified System Administrator Enterprise Linux 6 o superior**

El **INSTITUTO** podrá solicitar en cualquier momento del proceso de contratación y durante la vigencia del contrato, los originales de las certificaciones presentadas por el **LICITANTE** para su cotejo, mismas que serán devueltas una vez concluida la revisión.

El **LICITANTE** deberá presentar al Instituto, a través de la Coordinación de Servicios de Infraestructura Tecnológica Institucional cita en Toledo 21 6to piso, 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 de 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, el plan de trabajo, 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 acorde a lo descrito en el anexo técnico 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, 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 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. Cláusulas y Cumplimientos

a. 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**.

ANEXOS
DIVISIÓN DE CONTRATOS

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 Servicios 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

- **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.

ANEXOS
DIVISIÓN DE CONTRATOS

8. Administradores del contrato

El administrador del Contrato será el Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional, mismo que conforme a sus atribuciones será el encargado 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 de la adjudicación del contrato, 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, así como al artículo 8 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

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.

11. Conformación de la Propuesta

Los participantes en la 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

ANEXOS
DIVISIÓN DE CONTRATOS

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 con 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 o traducción simple al español. 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 deben emplear el mismo orden y secuencia de temas que comprenden dichos documentos, 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.
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

ANEXOS
DIVISIÓN DE CONTRATOS

No	Entregable
	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 ganador para garantizar el cumplimiento de todas y cada una de las obligaciones estipuladas en el contrato adjudicado, deberá presentar fianza expedida por afianzadora debidamente constituida en términos de la Ley de Instituciones de Seguros y Fianzas, por un importe equivalente al 10% (diez por ciento) del monto máximo del contrato, sin considerar el impuesto al valor agregado, a favor del Instituto.

La garantía deberá presentarse dentro del término 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 4.24.4 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.

De conformidad con el Artículo 81, fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, la ejecución de la garantía de cumplimiento del contrato será divisible y se hará efectiva de manera 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.

13. Niveles de Servicio

El Servicio de Continuidad de la Nube IMSS 2022 se sujetará a los niveles de servicio establecidos en el apéndice respectivo del Anexo Técnico correspondiente.

14. Penas convencionales y Deductivas

- Las penas convencionales y deductivas se calcularán conforme a lo establecido en el Apéndice 6 "Métricas de Niveles de Servicio".
- 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:

ANEXOS
DIVISIÓN DE CONTRATOS

- 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.

16. Ubicaciones para la prestación del servicio

El **LICITANTE** adjudicado tiene la obligación de prestar sus servicios en las 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 este 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

Se efectuarán pagos a "EL PROVEEDOR" una vez proporcionado los servicios, de conformidad con lo dispuesto en los artículos 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 93 de su Reglamento, así como por lo establecido en los Términos y Condiciones que se agreguen al contrato.

El pago del servicio se realizará en "EL INSTITUTO", cuyos domicilios se relacionan en el Anexo correspondiente del contrato, una vez que el servicio haya sido proporcionado conforme al anexo técnico:

El pago se realizará en pesos mexicanos, en los plazos normados por la Dirección de Finanzas en el "Procedimiento para la recepción, glosa v 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 áreas de trámite de erogaciones la representación impresa del Comprobante Fiscal Digital por Internet (CFDI), siempre y cuando se cuente con la suficiencia presupuestal, así como con la documentación comprobatoria que acredite la prestación de los servicios, y se indique en dicha documentación los servicios proporcionados, número de proveedor, número de contrato, número de fianza y denominación social de la afianzadora, en su caso.

"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 IMS471231I45, domicilio en Avenida Paseo de la Reforma número 476, Colonia Juárez, Código Postal 06600, Demarcación Territorial Cuauhtémoc, en la Ciudad de México.

"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".

ANEXOS
DIVISIÓN DE CONTRATOS

En ningún caso se deberá autorizar el pago de los servicios, 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 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". (En caso de aplicar)

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 (en caso de aplicar).

Para que "EL PROVEEDOR" pueda celebrar un contrato de cesión de derechos de cobro, deberá notificarlo por escrito a "ELINSTITUTO" 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 SS 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, o ante la Jefatura de Servicios de Finanzas o de la UMAE correspondiente. (Eliminar lo marcado cuando el pago se efectúe a Nivel Central o ante los Órganos de Operación Administrativa Desconcentrada).

El pago de los servicios 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.

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.

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

ANEXOS
DIVISIÓN DE CONTRATOS

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.

6. Si la aplicación de las penas convencionales rebasa el monto de la garantía de cumplimiento del contrato.

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).

20. Criterio de evaluación.

Para la evaluación de las propuestas se aplicará el criterio de evaluación binario, de acuerdo con lo establecido en el artículo 36 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en relación con el diverso 51 de su Reglamento.

Asimismo, al tratarse de un procedimiento de Adjudicación Directa y dado que las características técnicas del servicio están perfectamente definidas, resulta innecesario ponderarlas individualmente, ya que la falta de alguna de ellas afectaría la calidad del servicio en su totalidad.

21. Licencias, permisos, registros, certificados o autorizaciones que debe cumplir o aplicarse al bien o servicio a contratar.

No aplica.

22. Folletos, catálogos, fotografías, manuales entre otros, en caso de que se requieran para comprobar las especificaciones técnicas requeridas.

No aplica.

23. Visitas a las instalaciones institucionales, donde se suministrarán o colocarán los bienes o donde se prestarán los servicios, en su caso.

En caso de requerirse, el licitante podrá solicitar al instituto la visita a las instalaciones institucionales, donde se suministrarán o colocarán los bienes o donde se prestarán los servicios con al menos 5 días de anticipación a su visita.

24. En su caso, mecanismos requeridos al proveedor para responder por defectos o vicios ocultos de los bienes o de la calidad de los servicios.

No aplica.

25. Responsabilidad

ANEXOS
DIVISIÓN DE CONTRATOS

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 juridico.

26. 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).

27. Firmas de elaboración, revisión y aprobación

Elaboró	Cargo	Firma	Fecha
Héctor Javier Reyes Oropeza	Titular de la División de Administración de Centros de Datos.		06/05/2022

Revisó	Cargo	Firma	Fecha
Javier cortés López	Titular de la Coordinación Técnica de Operación Administración de Centro de Datos		06/05/2022

Aprobó	Cargo	Firma	Fecha
Eduardo Oropeza Ortiz	Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional		06/05/2022

IMSS	INSTITUTO MEXICANO DEL SEGURO SOCIAL DIRECCIÓN DE ADMINISTRACIÓN UNIDAD DE ADQUISICIONES COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS	Contrato Número S2M0117

ANEXO 2 (DOS)

"PROPUESTA TÉCNICA, APÉNDICES, PROPUESTA ECONÓMICA Y OFICIO DE NOTIFICACIÓN DE ADJUDICACIÓN"

EL PRESENTE ANEXO CONSTA DE **124** HOJAS INCLUYENDO ESTA CARÁTULA

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

DocuSign Envelope ID: 658B6DB9-3AF3-424C-8656-941FE346D1BF

Anexo Técnico

SGMP_Anexo Técnico

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

Ciudad de México a 13 de abril de 2022

Esta información es propiedad de Sixsigma Networks México, S.A. de C.V. (KIO NETWORKS), se proporciona con el carácter de confidencial. Esta información no será reproducida, usada o divulgada total o parcialmente por cualquier razón diferente que la de evaluar la propuesta de Servicios de KIO NETWORKS.

ANEXOS
DIVISIÓN DE CONTRATOS

ÍNDICE

1 OBJETIVO DEL DOCUMENTO 3
2 OBJETIVO 3
3 ALCANCE 3
4 REQUERIMIENTOS TECNICOS 4
4.1 Servicio de Continuidad Operativa y Soporte a la Operación 6
4.2 Servicio de Continuidad y Soporte de la Operación de Telecomunicaciones 7
4.3 Servicio de Continuidad y Soporte de Seguridad 7
4.4 Migración del Centro de Datos Actual al Centro de Datos Ofertado por el Licitante 8
5 PRUEBAS 13
6 PERFIL DEL PROVEEDOR 14
7 CONDICIONES TECNICAS DE ACEPTACION DE ENTREGABLES 16
8 CRONOGRAMA DE ACTIVIDADES 16
9 NIVELES DE SERVICIO ACORDADOS QUE DEBERAN CUMPLIRSE 20
9.1 Definición General de Entrega 21
9.2 Reportes del Servicio 21
9.3 Objetivos y Métricas especificas de Niveles de Servicio 23
10 REQUERIMIENTOS DE ARQUITECTURA TECNOLOGICA 24
11 RESTRICCIONES E INTERFACES CON OTROS ELEMENTOS 25
12 FIRMAS DE ELABORACION, REVISION Y APROBACION 25

KIO Networks

DS DS

1 OBJETIVO DEL DOCUMENTO

Elaborar el documento que contenga los requerimientos y las especificaciones técnicas y de calidad, así como el alcance de la adquisición, arrendamiento o servicio de TIC y SI que se pretenda contratar.

Clasificador Único de las Contrataciones Públicas (CUCOP): 31900004 Servicios a centros de datos (hospedaje, electricidad, video vigilancia, monitoreo, aire acondicionado, servidores y otros).

2 OBJETIVO

Contratar el **"Servicio de Continuidad de la Nube IMSS 2022"** con el fin de mantener los niveles de servicio proporcionados por el centro de datos actual que brinda la continuidad operativa de los sistemas de alcance nacional del Instituto Mexicano del Seguro Social.

3 ALCANCE

Sixsigma Networks S.A. de C.V. en lo consecutivo **KIO Networks** brindará continuidad operativa, soporte, gestión de la operación de los servicios, aplicaciones y componentes que permiten al Instituto disponer de las capacidades de infraestructura de procesamiento, almacenamiento, respaldo, comunicaciones, seguridad, plataformas tecnológicas y software en infraestructura que será consumida bajo demanda de acuerdo a las necesidades del Instituto, la cual no contará con anuncios de fin de venta o de soporte durante la vigencia del contrato, que hoy en día se encuentran desplegadas en las siguientes ubicaciones:

- CDP - Centro de Datos Primario (Ambientes Productivos y no Productivos)
- ENP - Extensión de Nube Privada (ATOM)
- SDI - Servicios desplegados en Instalaciones designadas por el Instituto

Toda la infraestructura que provee **KIO Networks** al Instituto se brinda en modo de servicio, los cuales cumplen con los niveles de servicios establecidos por el Instituto para cada uno de los servicios.

Centro de Datos Primario

El Instituto habilitará los mecanismos idóneos para garantizar la continuidad operativa, soporte y gestión de la operación de la infraestructura actual del centro de datos primario (aplicaciones, servicios, infraestructura de procesamiento, almacenamiento y respaldo, infraestructura de seguridad y telecomunicaciones), en tanto se lleva a cabo la migración del Centro de Datos Actual a la infraestructura del Centro de Datos ofertado por **KIO Networks** adjudicado, garantizando la operación de los aplicativos, servicios e infraestructura, de acuerdo a los niveles de servicio establecidos 99.982% de disponibilidad.

Extensión de Nube Privada (ATOM)

KIO Networks, brindará continuidad del servicio, soporte y gestión de la operación 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.

KIO Networks®

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

Servicios desplegados en instalaciones designadas por el Instituto

KIO Networks, brindará continuidad del servicio, soporte y gestión de la operación de infraestructura, por ejemplo, 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.

Ambientes no productivos en el Centro de Datos

KIO Networks, brindará continuidad operativa, soporte y gestión de la operación de la infraestructura actual del centro de datos que contenga ambientes no productivos (aplicaciones no productivas, servicios, infraestructura de procesamiento, almacenamiento y respaldo, infraestructura de seguridad y telecomunicaciones), así como su migración del Centro de Datos Actual a la infraestructura del Centro de Datos ofertado por **KIO Networks**, garantizando la operación de los aplicativos, servicios e infraestructura, de acuerdo a los niveles de servicio establecidos 99.982% de disponibilidad.

Comunicaciones

KIO Networks brindará la continuidad operativa, soporte y gestión de la operación de la solución de telecomunicaciones, incluyendo acciones para habilitación de infraestructura de conectividad en red con la funcionalidad de "Punto Neutro" durante el primer semestre del servicio, la cual deberá tener la capacidad de concentrar los enlaces de telecomunicaciones de las diferentes redes de telecomunicaciones del IMSS y proporcionadas por diversos prestadores de servicio, así como los enlaces de telecomunicaciones de los principales organismos públicos y privados con los que el Instituto interactúa. El servicio debe incluir la conectividad actual de 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.

KIO Networks brindará la continuidad a los servicios, aplicativos, servicios digitales y de información, así como su interconexión con los centros de datos propios del Instituto o del Gobierno Federal y entidades externas (tales como: SAT, RENAPO, Procesar, Banco de México, INFONAVIT, Bancos, Instituto Nacional Electoral, Afores, CONSAR, entre otros) que permitan el intercambio de información, conforme a los estándares de telecomunicaciones y seguridad definidos por el Instituto.

4 REQUERIMIENTOS TECNICOS

KIO Networks brindará continuidad operativa, soporte y gestión de la operación de la solución de infraestructura de procesamiento, almacenamiento, respaldos, telecomunicaciones y seguridad, así como a las aplicaciones, componentes y servicios digitales del Instituto en sus diversos esquemas desplegados, tales como: Centro de Datos Actual, Nodo de Extensión de Nube y Ubicaciones designadas por el Instituto, así como las que el Instituto designe durante la vigencia del Servicio.

Los servicios requeridos por el Instituto y que **KIO Networks** proveerá durante la vigencia del servicio son los siguientes:

- Servicio de Continuidad Operativa y Soporte
- Servicio de Continuidad y Soporte de Telecomunicaciones

DS JCHV DS JAR

- Servicio de Continuidad y Soporte de Seguridad

Para cada servicio antes mencionado, **KIO Networks** integrará como parte de la ejecución del servicio, los esquemas de Gestión de la Operación y Soporte, así como el Aprovisionamiento de infraestructura bajo demanda relativa a procesamiento, almacenamiento, respaldos, telecomunicaciones y seguridad.

La siguiente tabla muestra de manera enunciativa más no limitativa el esquema de organización de cada servicio:

Nombre del Servicio	Continuidad y Soporte bajo demanda	Aprovisionamiento de Infraestructura bajo demanda
Servicio de Continuidad Operativa y Soporte a la Operación	Servicios bajo demanda de continuidad operativa, gestión de la operación y soporte de la infraestructura de procesamiento, almacenamiento y respaldos, así como a las aplicaciones, componentes y servicios digitales del Instituto en cualquiera de sus capas (web, aplicativa, base de datos, balanceo etc.)	Aprovisionamiento de infraestructura de procesamiento, almacenamiento y respaldos, bajo demanda.
Servicio de Continuidad y Soporte de Telecomunicaciones	Servicios bajo demanda de continuidad operativa, gestión de la operación y soporte referente a componentes e infraestructura de telecomunicaciones, así como la interconexión entre los diferentes ecosistemas Institucionales, así como con otras entidades públicas y privadas.	Aprovisionamiento de infraestructura de telecomunicaciones, bajo demanda.
Servicio de Continuidad y Soporte de Seguridad	Servicios bajo demanda de continuidad operativa, gestión de la operación y soporte referente a componentes e infraestructura de seguridad física y lógica.	Aprovisionamiento de infraestructura de seguridad, bajo demanda.

KIO Networks proveerá el soporte técnico en caso de falla en un esquema de 7 días 24 horas durante la vigencia del servicio.

A continuación, se describe el objetivo de cada servicio requerido por el Instituto y que **KIO Networks** brindará como parte de los servicios.

Para efectos del anexo técnico y sus apéndices se entenderá como Bloque de Construcción Fundamental (BCF) a cualquier componente mínimo tecnológico de Infraestructura.

ANEXOS
DIVISIÓN DE CONTRATOS

4.1 Servicio de Continuidad Operativa y Soporte a la Operación

KIO Networks brindará continuidad operativa, gestión de la operación, habilitación de infraestructura, afinación, puesta a punto, configuración y soporte a los componentes de infraestructura de procesamiento, almacenamiento y respaldos, así como 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.

En el **Apéndice "Relación de Infraestructura Actual en Centro de Datos"** se encuentra la relación de los componentes e infraestructura de procesamiento, almacenamiento y respaldos, así como de telecomunicaciones y seguridad en el actual centro de datos, mismos que **KIO Networks** incluye para brindar continuidad operativa, soporte y servicio a los sistemas, aplicaciones, plataformas e infraestructura de procesamiento, almacenamiento y respaldos.

KIO Networks proporcionará el soporte en sitio para los Puntos de Acceso a la Nube cuando el Instituto lo requiera para lo cual, **KIO Networks** mantendrá el modelo de operación actual para los 4 hospitales que forman parte del Centro Médico Nacional de Occidente en Guadalajara, Jalisco. Cada ENP deberá soportar cuanto menos 400 Puntos de Acceso a la Nube (PAN) y 1,200 Escritorios en la Nube (EN), previendo un crecimiento una capacidad máxima de hasta 1000 PANs y 2000 ENs.

En el **Apéndice "Descripción Detallada de los Servicios de Continuidad de Nube IMSS"** se encuentra el detalle de los componentes:

- **Soporte a la Continuidad Operativa**
  - Gestión de eventos, requerimientos, incidentes, problemas, cambios, configuraciones y liberaciones.
  - Mesa de Servicio
- **Soporte y Gestión de la Operación**
  - Administración de Sistemas Operativos
  - Administración de Bases de Datos
  - Administración de Middleware
- **Soluciones Tecnológicas**
  - Monitoreo
  - Soporte de fabricante
  - CMDB

Durante la vigencia del servicio, el Instituto podrá solicitar procesos de migración de aplicaciones, servicios, e infraestructura, desde el Centro de Datos de **KIO Networks**, hacia los Centros de Datos propios del Instituto o del Gobierno Federal, en un esquema de continuidad operativa o de recuperación ante una contingencia o desastre, por lo cual **KIO Networks** participará en la definición de necesidades tecnológicas y proveerá de personal especializado para su ejecución y para mantener la continuidad operativa durante el proceso de migración mencionado, proporcionando todas las facilidades necesarias, tales como: configuraciones, accesos supervisados (sistemas operativos, middleware, bases de datos, virtualizadores, entre otros), arquitecturas o lo que el Instituto determine sea requerido respetando las normas de seguridad y de operación del Centro de Datos origen.

Para lo anterior **KIO Networks** proporcionará todas las facilidades necesarias para llevar a cabo dicha migración previo análisis de riesgos en el marco de lo establecido en las normas ISO 27001, incluyendo de manera enunciativa más no limitativa lo siguiente:

- Proporcionar acceso supervisado (si es necesario con usuarios administradores) a los equipos e infraestructura de procesamiento, almacenamiento, respaldo, infraestructura de telecomunicaciones y seguridad.
- Proporcionar archivos, configuraciones, ejecución de comandos, extracción de información de la infraestructura de procesamiento, almacenamiento y respaldo, infraestructura de telecomunicaciones y seguridad.
- Proporcionar respaldos, exportaciones, imágenes o elementos similares de los aplicativos o servicios, máquinas virtuales o elementos de infraestructura que permitan el análisis, para instalación, configuración, puesta a punto, o en su caso importación/exportación en Centro de Datos alterno que el Instituto designe para tal fin.
- Permitir la Instalación de agentes en los equipos que se encuentren en el Centro de Datos de **KIO Networks** para la extracción, monitoreo, exportación o cualquier componente tecnológico o configuración que el Instituto requiera.
- Proporcionar acceso a los ambientes tecnológicos origen, a fin de realizar la exportación, copiado, clonación o el procedimiento de migración que el Instituto determine.

4.2 Servicio de Continuidad y Soporte de la Operación de Telecomunicaciones

KIO Networks brindará continuidad operativa, gestión de la operación, habilitación de infraestructura, afinación, puesta a punto, configuración y soporte a los componentes de infraestructura de Telecomunicaciones.

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 Extensión de Nube Privada (ENP) y 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.

En el **Apéndice "Descripción Detallada de los Servicios de Continuidad de Nube IMSS"** se encuentra el detalle de los componentes para el Servicio de Continuidad y Soporte a la Operación de Telecomunicaciones:

- Servicio de Soporte de Extensión de Nube Privada
- Punto Neutro
- Servicios de Conectividad y Comunicaciones

4.3 Servicio de Continuidad y Soporte de Seguridad

KIO Networks brindará continuidad operativa, gestión de la operación, habilitación de infraestructura, afinación, puesta a punto, configuración y soporte a los componentes de infraestructura de Seguridad.

KIO Networks brindará el servicio de Centro de Operaciones de la Seguridad (SOC), que se encuentra físicamente en las instalaciones de **KIO Networks**. **KIO Networks** brindará la gestión de la seguridad y será responsable de la

ANEXOS
DIVISIÓN DE CONTRATOS

administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad, ejecución actividades de revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, así como el establecimiento de acciones de mejora continua.

En el **Apéndice "Descripción Detallada de los Servicios de Continuidad de Nube IMSS"** se encuentra el detalle de los componentes para el Servicio de Continuidad y Soporte de Seguridad:

- Centro de Operaciones de la Seguridad (SOC)
- Administración y Soporte de Componentes de Seguridad

A continuación, se describen los servicios adicionales para el "Servicio de Continuidad de la Nube IMSS 2022", mismos que **KIO Networks** deberá incluir como:

4.4 Migración del Centro de Datos Actual al Centro de Datos Ofertado por el Licitante

KIO Networks al contar con los servicios actuales en el centro de datos, brindara continuidad a los servicios del instituto sin necesidad de migración, por lo que este apartado se ejecuta como un proceso administrativo sin necesidad de un plan de trabajo para las actividades de migración, y se muestra en el FOCON como un día de migración y un peso mexicano de costo de migración.

A continuación, se describen los principales **requerimientos funcionales y no funcionales** que **KIO Networks** cumplirá para la entrega de los servicios objeto del presente anexo técnico, términos y condiciones, así como los apéndices correspondientes:

a) **Funcionales**

Modelos de Entrega o Despliegue del Servicio

KIO Networks desplegará los servicios descritos en el presente anexo en las siguientes modalidades de entrega o despliegue del servicio.

Servicio	Modalidad de entrega o despliegue del servicio
Servicio de Continuidad Operativa y Soporte a la Operación	• Centro de Datos Primario • Ambientes productivos y No productivos • Servicios desplegados en Instalaciones designadas por el Instituto • Extensión de Nube Privada (ATOM)
Servicio de Continuidad y Soporte de Telecomunicaciones	• Centro de Datos Primario
Servicio de Continuidad y Soporte de Seguridad	• Centro de Datos Primario • Servicios de seguridad a nivel nacional

b) **No funcionales**

Disponibilidad y niveles de servicio

KIO Networks proporcionará los servicios objeto del presente anexo técnico y apéndices respectivos, en un esquema de disponibilidad del **99.982%** durante la vigencia del contrato y efectuar las acciones necesarias para que se encuentren operando y sean accesibles para el Instituto alineándose a la normatividad en la materia durante la vigencia del servicio y buenas prácticas que señala la industria, en cada uno de sus componentes y procesos del ciclo de vida de entrega del servicio.

KIO Networks efectuará acciones, vigilancia de los servicios y entregar mensualmente propuestas de mejora acorde a los siguientes rubros que de manera enunciativa más no limitativa se describen:

- Vigilar la disponibilidad de los componentes de la infraestructura de TIC que soportan los servicios del presente anexo técnico, incluidos de ser posible los relacionados que sean proporcionados por terceros.
- Informar de riesgos que pudieran materializarse al efectuar adecuaciones a los componentes de la infraestructura que soportan los servicios.
- Reporte de 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 monitoreo del servicio y gestionadas por cualquiera de los servicios:
    - Servicio de Continuidad Operativa y Soporte a la Operación
    - Servicio de Continuidad y Soporte de Telecomunicaciones
    - Servicio de Continuidad y Soporte de Seguridad
- Cumplimiento de los niveles de disponibilidad de los servicios y de los componentes de la infraestructura con respecto a:
    - Los niveles de servicio originalmente acordados.
    - Los niveles de servicio efectivamente proporcionados.
- Configuración en una base de datos de gestión de configuraciones (CMDB) y las características de cada componente de la infraestructura que soportan los servicios que permita correlacionar incidentes y su impacto.
- Niveles de servicio alcanzados.
- Requerimientos, actuales y previstos, de disponibilidad de los servicios objeto del presente Anexo Técnico.

Gestión de la Base de Datos de Configuraciones

KIO Networks habilitará, configurará, pondrá a punto, actualizará, brindará continuidad y dará soporte a la base de datos de configuraciones (CMDB) e integrará la información de los elementos de configuración (CI) de la infraestructura objeto del presente anexo técnico.

ANEXOS
DIVISIÓN DE CONTRATOS

KIO Networks presentará un plan de trabajo para mantener actualizada la información de los elementos de configuración (CI) de manera periódica. El plan de trabajo de la CMDB deberá ser revisado y aprobado por el Instituto en las mesas de trabajo semanales.

La solución de la CMDB que habilite **KIO Networks** proveerá mecanismos que permitan la consulta de información al personal designado por el Instituto. Los mecanismos de consulta podrán ser de manera enunciativa mas no limitativa los siguientes:

- API (Application Programming Interface)
- Página web de consulta de información.
- Exportación de los elementos de configuración y su relación.

Durante la vigencia del contrato de manera mensual y al término del contrato, **KIO Networks** entregará toda la información de la CMDB al Instituto en un medio electrónico que permita su exportación/importación.

La CMDB habilitada por **KIO Networks** es utilizada por el Instituto para correlacionar eventos e incidentes y determinar la infraestructura susceptible de impacto colateral, esto es, en caso de un incidente y que por causa de la falla de un componente se vean afectados otros activos tecnológicos, en virtud de que no puedan ser ingresados o utilizados hasta el incidente inicial sea corregido. En esos casos, se aplicarán deductivas al componente afectado y a toda la infraestructura susceptible de impacto colateral.

KIO Networks designa a un **coordinador de configuraciones**, quien tendrá las siguientes actividades enunciativas más no limitativas: administración, configuración, actualización de la CMDB, así como notificación al Instituto los cambios realizados.

KIO Networks entregará y explicará al Instituto de manera mensual un reporte de gestión de configuraciones que soporte las acciones referentes a este apartado, es decir, los cambios efectuados en el mes, incluyendo la infraestructura susceptible de impacto colateral.

Gestión del conocimiento

KIO Networks consolidará, entregará y explicará mensualmente la información relacionada al servicio y permitir al Instituto acceder a las bases del conocimiento y repositorios, mismos que deberán contener de manera enunciativa más no limitativa al menos lo siguiente:

- Memorias técnicas de instalación, distribución, configuración, partición y asignación de la infraestructura física y virtual.
- Manejo y operación de las herramientas de monitoreo, destacando los cambios efectuados desde la última reunión.
- Memorias técnicas de instalación, distribución, configuración y puesta a punto del Sistema Operativo, Bases de Datos, Software propietario y Open Source, capa aplicativa y todos aquellos componentes instalados para la operación de los aplicativos o servicios del instituto.
- Memorias Técnicas de la instalación, distribución, configuración y puesta a punto de los componentes habilitados para proporcionar la conectividad de la red para los aproximadamente 3,000 inmuebles del IMSS donde interoperan con los sistemas y aplicativos ubicados en los Centros de datos centralizados o con organismos terceros, incluyendo el "Punto Neutro".

- Memorias técnicas de los cambios realizados en los componentes con motivo de mejoras en el desempeño de los mismos o bien como resultado de la atención a incidentes, problemas, cambios.
- Memorias técnicas de la solución a incidentes y base de datos de errores conocidos.
- Base de Datos de Administración de Configuraciones.
- Memorias técnicas de los procesos de migración.
- Información, memorias, configuraciones o cualquier activo requerido por el Instituto definido en las mesas de trabajo semanales.

KIO Networks brindará acceso al Instituto a las bases del conocimiento relacionado con los servicios y entregar copia de dichas bases de conocimiento en medio electrónico cada mes, junto con los trámites de facturación correspondientes.

KIO Networks efectuará la transferencia de conocimiento, en los cuales personal del **LICITANTE** compartirá a personal del IMSS todo lo relacionado a la gestión de la operación y soporte de la infraestructura y servicios.

Actualización Tecnológica para Contenedores (Microservicios)

KIO Networks participará en conjunto con el Instituto en la definición y ejecución de la estrategia de migración que habilite el consumo de Contenedores (Microservicios) durante la vigencia del servicio.

El Instituto requiere efectuar acciones para que el 33% de los servicios Institucionales del ecosistema aplicativo sea susceptible de contenerizar a microservicios. Por ello de manera conjunta, el Instituto y **KIO Networks** deberán contar con las capacidades necesarias en términos de recursos humanos, procesos de operación e infraestructura de TI para colaborar en el cumplimiento de esta estrategia y lograr la transformación y modernización de los servicios tecnológicos que el IMSS ofrece a sus derechohabientes y al público en general.
De manera conjunta, el Instituto y **KIO Networks** deberán definir un modelo de gobierno para la actualización a contenedores (microservicios) que incluya de manera enunciativa más no limitativa: Esquemas de desarrollo, Políticas de Operación, Procesos, Métricas y Desempeño que regirán la forma de trabajar en los distintos proyectos que requieran ser administrados con una cultura de Integración Continua y Desarrollo Continuo para la migración a contenedores (microservicios) incluyendo el manejo y operación del pipeline.

De manera conjunta, el Instituto y **KIO Networks** definirán arquitecturas operativas, las cuales serán notificadas a las distintas áreas técnicas del Instituto, a fin de que sean atendidas y utilizadas por las distintas fábricas de software y áreas de desarrollo del Instituto.

Grupo de Gobierno del Contrato

El Grupo de Gobierno del Contrato estará conformado por los responsables de los siguientes servicios:

Servicio	Integrantes
Servicio de Continuidad Operativa y Soporte a la Operación	Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional Titular de la Coordinación Técnica de Administración de Centro de Datos

ANEXOS
DIVISIÓN DE CONTRATOS

	Titular de la División de Administración de Centros de Datos.
Servicio de Continuidad y Soporte de Telecomunicaciones	Titular de la Coordinación Técnica de Telecomunicaciones
Servicio de Continuidad y Soporte de Seguridad	Titular de la División de Seguridad Informática

Los miembros del Grupo de Gobierno del Contrato (GGC) 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, cambios, eventos, problemas, y cualquier información relacionada al servicio prestado.

KIO Networks efectuará e informará mensualmente al GGC del Instituto el seguimiento de cada servicio, informando avances, estado de requerimientos, asuntos, consumos, riesgos, desviaciones, incidentes, cambios, eventos, problemas e información relacionada al servicio prestado tales como: memorias técnicas de instalación configuración y puesta a punto de los aplicativos, ejercicio presupuestal detallado por servicio, infraestructura, proyección del gasto, aplicativo, planes de actualización tecnológica, arquitectura por aplicativo, CMDB, detalle del licenciamiento instalado y distribución por aplicativo, fechas de vencimiento de los certificados, proyección de crecimiento por aplicativo, capacidad de la infraestructura y memorias técnicas de las migraciones ejecutadas al inicio y durante la vigencia del servicio.

KIO Networks avisará de manera inmediata al responsable del GCC del servicio afectado, al momento de presentarse un evento o incidente que afecte la operación de algún(os) servicios, sistemas o aplicativos Institucionales, así como entregar un análisis e informe detallado del evento (Postmortem) a las 48 horas después de concluido el incidente.

KIO Networks 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 de toda la información que se desprenda del presente anexo técnico. **KIO Networks** expondrá y explicará el contenido de dicho repositorio al Instituto, así mismo habilitará accesos a dicho repositorio para los miembros del GGC. Al término del contrato, **KIO Networks** transferirá al Instituto toda la información de dicho repositorio.

KIO Networks se apega 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.

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 mensualmente 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 GGC 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 GGC 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, **KIO Networks** presentará al GGC 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, presentará al GGC de manera mensual 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 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 infraestructura 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.

El IMSS en caso de contar con contratos de licenciamientos con distintos fabricantes (base de datos, sistema operativo o licenciamientos diversos), proporcionará a **KIO Networks** los datos requeridos para que **KIO Networks** a nombre del IMSS levante los tickets que en su caso se requieran a fin de solventar incidencias, eventos o actualizaciones. En el caso de que el Instituto no cuente con contratos de licenciamiento o en que esos contratos no sean suficientes para atender las necesidades institucionales, el Instituto podrá solicitar al **LICITANTE** que habilite el licenciamiento correspondiente en la modalidad de servicio administrado. Preferentemente se buscará utilizar los contratos de licenciamiento del IMSS.

KIO Networks definirá e implementará mecanismos de comunicación hacia los responsables de 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.

KIO Networks elaborará en un plazo no mayor a 10 días hábiles posteriores a la adjudicación del contrato, una matriz de los verbos, sujetos obligados, 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".

KIO Networks a partir de la matriz de verbos, deberá generar 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 habilitado por **KIO Networks** con acceso permanente a los administradores del contrato (grupo de gobierno del contrato) y deberá actualizarse, y presentarse de manera mensual en las juntas de gobierno del contrato.

5 PRUEBAS

ANEXOS
DIVISIÓN DE CONTRATOS

No se requiere la ejecución de procesos de prueba durante el procedimiento de contratación.

6 PERFIL DEL PROVEEDOR

KIO Networks cumple con las siguientes certificaciones de Centros de Datos así como, de Gestión del Servicio que se listan de manera enunciativa más no limitativa en la siguiente tabla:

Componente o Servicio	Descripción	Especificación	Tipo
Certificación de Centros de Datos	Certificación de Disponibilidad del Centro de Datos Ofertado	TIER III o ICREA IV equivalente o superior	Funcional
Gestión de Servicios de Tecnologías de la Información y Comunicaciones	Certificación de gestión de procesos de Tecnologías de la Información y Comunicaciones.	ITIL V3 equivalente o superior	Funcional
Sistemas de Gestión del Servicio	Calidad en la Gestión de Servicios de TIC	ISO/IEC 20000-1 equivalente o superior	Funcional
Gestión de Seguridad de la Información	Implementación, Mantenimiento y gestión de Sistemas de Gestión de Seguridad de la Información	ISO 27001 equivalente o superior	Funcional

KIO Networks acreditar 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.

KIO Networks entrega el documento vigente expedido por el SAT en el que se emite la opinión de cumplimiento de las obligaciones fiscales, positivo y vigente.

KIO Networks cuenta con experiencia comprobable de al menos 5 años para brindar los servicios objeto del presente anexo técnico, apéndices, así como términos y condiciones, para lo cual presenta copia de contratos, pedidos o convenios formalizados con el sector público o privado cuyo objeto esté relacionado con los servicios de la presente licitación.

KIO Networks cuenta con especialidad comprobable de al menos 5 contratos formalizados cuyo objeto está relacionado con la prestación de servicios similares al de la presente licitación.

Certificaciones enunciativas más no limitativas, o en su caso, similares en funcionalidad o tema en:

- **ISO/IEC 27001**
- **ISO/IEC 20000**
- **ITIL Expert Certificate**
- **ITIL Foundation Certificate in IT Service Management**
- **ITIL intermediate in Operational support and analysis**

KIO Networks

DS JCHV DS JAR

- **ITIL intermediate in Service Offering AND Agreements**
- **ITIL intermediate un Release, control and validación**

El Administrador de proyectos deberá contar con las siguientes certificaciones:

- **Project Management Institute (PMI)**
- **ITIL Foundation Certificate in IT Service Management version 4**
- **Scrum Certified Master**

KIO Networks cuenta con el personal certificado en Metodologías de Administración de Proyectos para la dirección del proyecto.

KIO Networks cuenta con el personal certificado o con experiencia comprobable en productos, software y componentes descritos en el presente anexo técnico por lo que deberá adjuntar a su propuesta las siguientes certificaciones:

- **CCNA - Cisco Certified Network Associate**
- **CCNA - Cisco Certified Network Associate Routing and Switching**
- **CCNP - Cisco Certified Network Professional**
- **Cisco Certified Specialist - Data Center Core**
- **CISM - Certified Information Security Manager**
- **CISSP Certified Information Systems Security Professional**
- **MCITP Enterprise Administrator on Windows Server 2008**
- **MCTS Microsoft Exchange Server 2007 Configuration**
- **Scrum Master Certified Credential**
- **Exchange Server 2007 Configuration**
- **Windows Server 2008 Active Directory, Configuring**
- **Windows Server 2008 Applications Infrastructure, Configuring**
- **Windows Server 2008 Network Infrastructure, Configuring**
- **Windows Server 2008, Enterprise Administrator**
- **Microsoft SQL Server 2008, Implementation and Maintenance**
- **Oracle Certified Associate - Oracle WebLogic Server 11g System Administrator**
- **Oracle Database 11g: Administrator Certified Associate**
- **Oracle Database 11g: Administrator Certified Professional**
- **Oracle Database 12c Certified Implementation Specialist**
- **Oracle WebLogic Server 12c Administrator**
- **Oracle VM 3.0 for x86 Certified Implementation Specialist**
- **VMware Certified Professional Data Center Virtualization 2019 o superior**
- **Querying Microsoft SQL Server 2012/2014 o superior**
- **Administering Microsoft SQL Server 2012/2014 Databases**
- **Implementing a Data Warehouse with Microsoft SQL Server 2012/2014**
- **Microsoft Certified Solutions Associate SQL Server 2012/2014**
- **Red Hat Certified System Administrator Enterprise Linux 6 o superior**

El **INSTITUTO** podrá solicitar en cualquier momento del proceso de contratación y durante la vigencia del contrato, los originales de las certificaciones presentadas por **KIO Networks** para su cotejo, mismas que serán devueltas una vez concluida la revisión.

ANEXOS
DIVISIÓN DE CONTRATOS

KIO Networks presentará al Instituto, a través de la Coordinación de Servicios de Infraestructura Tecnológica Institucional cita en Toledo 21 6to piso, 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 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, el plan de trabajo, 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 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 acorde a lo descrito en el anexo técnico y con los que el Instituto estará colaborando, su cargo y puesto, así como los datos y la vía de comunicación para contactarlo.

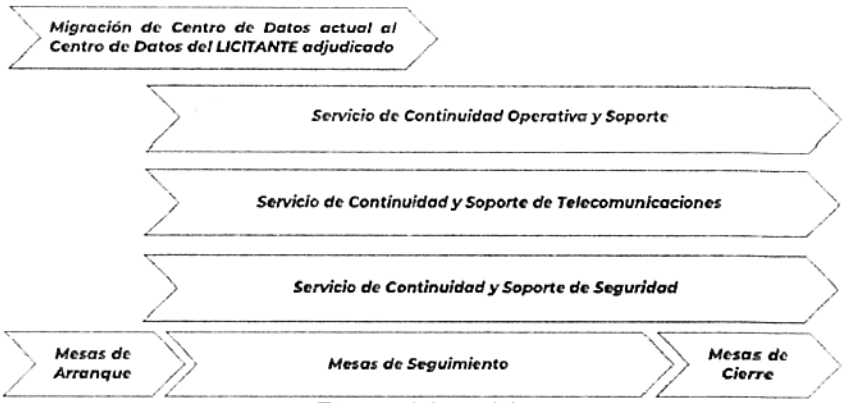
7 CONDICIONES TECNICAS DE ACEPTACION DE ENTREGABLES

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.

8 CRONOGRAMA DE ACTIVIDADES

KIO Networks entregará el plan de trabajo estableciendo actividades, responsables, tiempos para dar cumplimiento de las obligaciones relacionadas a los servicios del presente anexo técnico.

La siguiente imagen se mencionan las etapas principales del plan de trabajo que incluye:



Etapas del servicio

KIO Networks incluye en la propuesta el Plan de Trabajo especificando de manera detallada hitos y fases para el cumplimiento de cada una de las etapas y servicios objeto del presente anexo técnico. El plan de trabajo presentado por **KIO Networks**, integra información a detalle para los servicios siguientes:

- Servicio de Continuidad Operativa y Soporte
- Servicio de Continuidad y Soporte de Telecomunicaciones
- Servicio de Continuidad y Soporte de Seguridad

KIO Networks incluye el detalle para la etapa de **Migración del Centro de Datos Actual al Centro de Datos ofertado.**

El plan de trabajo presentado por **KIO Networks** incluye el esfuerzo de trabajo detallado de cada bloque de trabajo que integren los servicios, incluir duración de las etapas importantes dimensionando los tiempos de afectación, que permitan al Instituto evaluar técnica y funcionalmente la viabilidad del plan de trabajo.

A continuación, se especifica de manera enunciativa más no limitativa, los principales hitos, indicando fase, identificador, descripción del hito, las fechas relativas y absolutas de inicio y/o término y cantidad de días naturales máximos.

Tabla Hitos relevantes a considerar en el Plan de trabajo

Fase	ID	Hito	Inicio / Término Máximo del Hito	Máxima duración en días naturales*	Precedente(s)
Proceso de Migración de Centro de Datos actual al Centro de Datos ofertado por **KIO Networks**					
Planeación del Arranque	1	Kick-Off y presentación del equipo de trabajo de **KIO Networks**.	A más tardar 3 días naturales posteriores al Fallo	Plazo ofertado por **KIO Networks**	N/A

ANEXOS
DIVISIÓN DE CONTRATOS

Fase	ID	Hito	Inicio / Término Máximo del Hito	Máxima duración en días naturales*	Precedente(s)
	2	Mesas (sesiones) de trabajo de Planeación del Arranque, entre **KIO Networks** y el IMSS, convocadas por el Grupo Administrador del Contrato IMSS	A más tardar 5 días naturales posteriores al Fallo	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 de arranque.	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 3 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 del presente anexo técnico.	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 al centro de datos del **LICITANTE** adjudicado.	6	Inicio de actividades de migración del centro de datos actual al centro de datos ofertado por **KIO Networks** incluyendo servicios de punto neutro y todo lo necesario para la operación de los servicios.	Al día natural siguiente a la aprobación, por parte del IMSS, del Plan de Trabajo Detallado	Plazo ofertado por **KIO Networks**	4

KIO Networks

DS JCHV DS JAR

Fase	ID	Hito	Inicio / Término Máximo del Hito	Máxima duración en días naturales*	Precedente(s)
	7	Estrategia de continuidad de servicios del Centro de Datos Actual durante el proceso de migración al centro de Datos ofertado por **KIO Networks**	Al día natural siguiente a la aprobación, por parte del IMSS, del Plan de Trabajo Detallado	Plazo ofertado por **KIO Networks**	4
	8	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
	9	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
	10	Inicio de los Servicios asociados a la continuidad operativa de los servicios del presente anexo técnico.	Plazo ofertado por **KIO Networks**	Plazo ofertado por **KIO Networks**	N/A
	11	Inicio de actividades de migración tecnológica hacia ambientes basados en contenedores	Plazo ofertado por **KIO Networks**	Plazo ofertado por **KIO Networks**	8
	12	Habilitación de ambientes en los Centros de Datos designados por el Instituto.	Plazo ofertado por **KIO Networks**	Plazo ofertado por **KIO Networks**	8
	13	Actividades de Finalización del Contrato.	A más tardar 4 meses naturales antes del día de la	31 de diciembre de 2022	N/A

KIO Networks

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

Fase	ID	Hito	Inicio / Término Máximo del Hito	Máxima duración en días naturales*	Precedente(s)
			Finalización del Contrato		
CIERRE	14	Finalización del Contrato	-	31 de diciembre de 2022	N/A

9 NIVELES DE SERVICIO ACORDADOS QUE DEBERAN CUMPLIRSE

KIO Networks cumplirá con el nivel de servicio requerido para los servicios de infraestructura de procesamiento, almacenamiento, respaldos, telecomunicaciones y seguridad, incluyendo aplicaciones, componentes, servicios digitales y todos elementos necesarios para su funcionamiento, conforme a la siguiente tabla:

Nivel de Disponibilidad	**Minutos indisponibles permitidos en el mes para los servicios del presente contrato** **A partir de este límite se aplicarán deductivas por prestación deficiente del servicio**
99.982%	7.8 minutos

KIO Networks habilitará, instalará, configurará, pondrá a punto y operará una solución o herramienta para medir los diferentes niveles de servicio de la infraestructura de procesamiento, almacenamiento, respaldos, telecomunicaciones y seguridad, incluyendo todos elementos necesarios para su funcionamiento. **KIO Networks** utilizará las herramientas habilitadas en el **Servicio de Continuidad a la Operación 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.

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.

KIO Networks proporcionará la transferencia de conocimiento y adiestramiento tecnológico necesario en el manejo y administración de las herramientas de niveles de servicio para el personal definido por el Grupo de Gobierno del Contrato, 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 y las mesas de trabajo semanales.

KIO Networks

DS JCHV DS JAR

El software para niveles de servicio propuesto por **KIO Networks** 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
- 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

9.1 Definición General de Entrega

KIO Networks dará cumplimiento a la entrega de los servicios acorde a las especificaciones, condiciones, tiempos de entrega definidos en el presente anexo, los servicios entregados serán validos por el Instituto cuando 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**).

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 específica, dedicada a los diferentes servicios del presente anexo técnico.

9.2 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 deberán ser 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:

ANEXOS
DIVISIÓN DE CONTRATOS

Num.	Nombre y Descripción	Frecuencia del reporte y fecha de entrega máxima a partir de la cual se aplicarán deductivas	Inicio de la Entrega
Reporte de Entrega del Servicio			
01	**Disponibilidad de los aplicativos**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
02	**Utilización y desempeño de la infraestructura**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
03	**Impacto a la operación en tiempo (minutos)**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
04	**Reporte de Gestión de Requerimientos**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
05	**Reporte de Gestión de Incidentes**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
06	**Reporte de Gestión de Problemas**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
07	**Reporte de Gestión de Configuraciones**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
08	**Reporte de Gestión de Cambios**	Se entregarán dentro de los primeros 05 días hábiles de cada mes devengado	Una vez iniciado el servicio
09	**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

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 **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 del presente anexo técnico, deberán ser 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.

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:

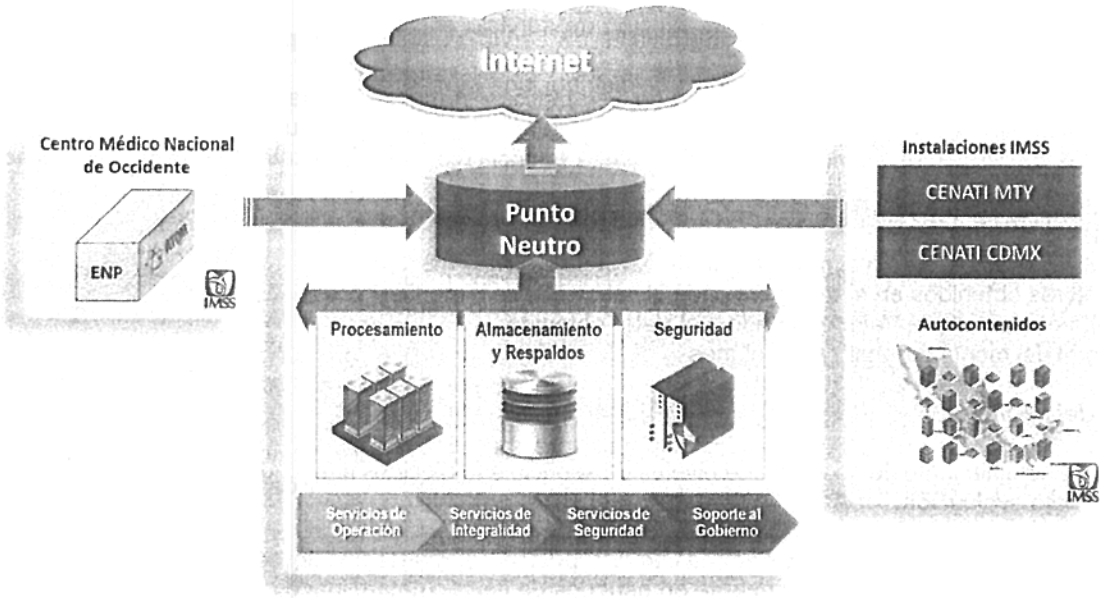
- Mes que se evalúa
- Cantidad total de acciones realizadas en el mes
- Cantidad total de acciones realizadas dentro de la ventana de tiempo establecida en el mes
- Anexo de relación de acciones realizadas, identificando su tipo, tiempo de inicio y finalización
- Valores esperados en el mes para cada 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.

9.3 Objetivos y Métricas especificas 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.

10 REQUERIMIENTOS DE ARQUITECTURA TECNOLOGICA

El modelo actual del ecosistema del Instituto con el cual se brindan los servicios a sus derechohabientes, patrones, jubilados, pensionado y público en general se muestra a continuación de manera conceptual:



KIO Networks considera en su propuesta técnica la complejidad del ecosistema que se ha construido bajo el concepto de arquitectura empresarial por lo menos en los 8 últimos años, Como se puede observar en la imagen anterior, los dominios tecnológicos que lo integran con más de 98,000 componentes de configuración atienden las diferentes necesidades operativas del Instituto y su interacción.

El criterio para considerar concluida la migración desde el Centro de Datos actual hacia el Centro de Datos ofertado, será en el momento en que se encuentren los servicios descritos anteriormente activos y operando en la infraestructura propuesta por el **KIO Networks**, e interactuando con el ecosistema tecnológico institucional, esto es; con los ambientes operativos digitales productivos y no productivos instalados en los diferentes centros de datos IMSS y del Gobierno Federal así como organismos con los que interactúa el Instituto tales como SAT, RENAPO, INFONAVIT, BANCO DE MÉXICO, PROCESAR, CONSAR, BANCOS Y AFORES, entre otros, validados de conformidad por el personal que el Instituto designe (áreas de telecomunicaciones y seguridad informática, infraestructura tecnológica, desarrollo, monitoreo así como el personal de las direcciones normativas que hacen uso de los servicios en los casos que aplique).

Por lo anterior **KIO Networks** realizar actividades técnicas complejas para migrar los servicios, aplicaciones y demás componentes al Centro de Datos propuesto incorporando en su modelo arquitectónico los elementos que garanticen la continuidad operativa del Instituto, los elementos de análisis para arquitectar la solución propuesta se encuentran en los apéndices "Componentes de Infraestructura" y "Apéndice Detalle de Servicios."

Asimismo, **KIO Networks** considera en su propuesta técnica los lineamientos establecidos en el ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, emitido por la Coordinación de Estrategia Digital Nacional, el pasado mes de septiembre de 2021.

11 RESTRICCIONES E INTERFACES CON OTROS ELEMENTOS

El Centro de Datos actual que provee **KIO Networks** intercambia información y ejecuta diversos procesos con diferentes ecosistemas y entidades privadas y públicas, tales como:

- Centros Nacional de Tecnologías de Información propiedad del Instituto (CENATI).
- Centro de Datos de Gobierno Federal en el Instituto Potosino de Investigación Científica y Tecnológica (IPICYT).
- Entidades externas (tales como: SAT, RENAPO, Procesar, Banco de México, INFONAVIT, Bancos, Instituto Nacional Electoral, Afores, CONSAR, entre otros)

Intercambio de información que el Instituto tiene de manera enunciativa mas no limitativa, son las siguientes:

Para el caso del Centro Nacional de Tecnologías de Información en Monterrey, se intercambia información de manera diaria para la actualización de información relacionada a asegurados, patrones, pensiones, para alimentar los procesos de Afiliación, Recaudación e Incorporación, así como Prestaciones económicas y Sociales.

Respecto al Instituto Potosino de Investigación Científica y Tecnológica, se tiene un modelo de intercambio de información entre las aplicaciones que se han desplegado en el centro de datos de gobierno federal y el centro de datos actual, para el consumo de servicios de vigencia de derechos, firma electrónica, bóveda y servicios transversales por parte de las aplicaciones que dan atención a la pandemia por COVID19, así como esquemas de replicación de bases de datos para las bases de datos de vacunas, vigilancia epidemiológica y base de datos transaccional única.

Finalmente, para las entidades externas públicas o privadas, el centro de datos actual que provee **KIO Networks**, tiene interconexión con los centros de datos propios del Instituto o del Gobierno Federal y entidades externas (tales como: SAT, RENAPO, Procesar, Banco de México, INFONAVIT, Bancos, Instituto Nacional Electoral, Afores, CONSAR, entre otros) para el intercambio de información, conforme a los estándares de telecomunicaciones y seguridad definidos por el Instituto.

12 FIRMAS DE ELABORACION, REVISION Y APROBACION

ANEXOS
DIVISIÓN DE CONTRATOS

Atentamente

DocuSigned by:
413DA356D32D4B3...

JUAN CARLOS MARTÍNEZ VALDÉS
REPRESENTANTE LEGAL
SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.

DS DS

DocuSign Envelope ID: 47B57195-AD1A-465D-B7B6-0950D030E160

Apéndice 1

Componentes de Infraestructura

SGMP_Apéndice_1

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

Ciudad de México a 13 de abril de 2022

Esta información es propiedad de Sixsigma Networks México, S.A. de C.V. (KIO NETWORKS), se proporciona con el carácter de confidencial. Esta información no será reproducida, usada o divulgada total o parcialmente por cualquier razón diferente que la de evaluar la propuesta de Servicios de KIO NETWORKS.

ANEXOS
DIVISIÓN DE CONTRATOS

ÍNDICE

1 OBJETIVO DEL DOCUMENTO 3
2 INFRAESTRUCTURA 3
2.1 Plataforma 3
2.1.1 Hardware 3
2.1.2 Sistema Operativo 12
2.1.3 Plataformas de Virtualización 13
2.1.4 Virtualización 16
2.2 Red 17
2.2.1 Zona 17
2.2.2 Pública 22
2.2.3 Infraestructura de Red 25
2.3 Instalaciones 26
2.3.1 Co-ubicación en modalidades de despliegue 26
3 APLICACIONES 27
3.1 Análisis estadístico 27
3.1.1 Sistema de Gestión de bases de datos 27
3.2 Herramientas y entorno de desarrollo 28
3.2.1 Entorno de desarrollo integrado (IDE) 28
3.2.2 Gestión de documentos y contenidos 28
3.3 Middleware 29
3.3.1 Bus de servicios empresariales (ESB) 29
3.4 Comunicación unificada y colaboración 31
3.4.1 Correo electrónico 31
4 OPERACIÓN DIGITAL 33
4.1 Servicios Generales 33
4.1.1 Gestión de la seguridad cibernética 33
4.1.2 Soporte para la entrega de servicios institucionales 34
3 FIRMAS DE ELABORACION, REVISION Y APROBACION 34

KIO Networks®

DS JCHV DS JAR

1 OBJETIVO DEL DOCUMENTO

El objetivo del presente Apéndice es establecer la descripción de los Componentes de Infraestructura referidos en el Anexo Técnico del Servicio Administrado objeto de esta Licitación

2 INFRAESTRUCTURA

2.1 Plataforma

2.1.1 Hardware

2.1.1.1 SERVIDORES DE MEDIO DESEMPEÑO

2.1.1.1.1 SERVIDOR X86 MODALIDADES CDP, ENP Y SDI

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

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.

ANEXOS
DIVISIÓN DE CONTRATOS

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

Los soportes para los sistemas operativos Oracle y Windows serán proporcionados por el Instituto, el Licitante deberá integrar en su propuesta el licenciamiento, así como el soporte para los productos Linux.

2.1.1.1.2 MODULO 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

2.1.1.2 MEDIOS DE ALMACENAMIENTO DE ACCESO DIRECTO

2.1.1.2.1 ALMACENAMIENTO DE DATOS INDIVIDUAL

KIO Networks dará 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 tendrá 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.

ANEXOS
DIVISIÓN DE CONTRATOS

- 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 **KIO Networks**, el contenido almacenado podrá regenerarse utilizando los niveles de protección solicitados.

El servicio cuenta 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

2.1.1.2.2 RESPALDO DE DATOS INDIVIDUAL

KIO Networks dará el servicio para el sistema de respaldos de Datos con las siguientes características:

- 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 permite la recuperación mediante snaps y clones

El equipo incluye todo el licenciamiento de software necesario para cumplir con los requerimientos

En caso de falla de algún componente del equipo utilizado el contenido almacenado puede regenerarse utilizando los niveles de protección solicitados.
El equipo cuenta 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.

2.1.1.2.3 UNIDAD DE ALMACENAMIENTO DE MEDIA CATEGORIA PARA APLICACIONES DE BAJO DESEMPEÑO

KIO Networks dará el servicio de almacenamiento de media categoría para almacenar todo lo correspondiente a equipos virtualizados, por lo que el equipo tiene las siguientes características:

• El equipo cuenta 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 tiene 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 tiene la capacidad de integración de protección de réplica en donde se alcance el valor de RPO =0
• El equipo tiene la capacidad de integración de replicación sobre IP a cualquier distancia y contar con protección durante falla de link WAN.
• El equipo tiene la capacidad de integración a replica donde se reduzcan costos de comunicación (anchos de banda)

El equipo incluye 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 asíncrono, 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 tecnología integrada para la optimización del almacenamiento mediante la compresión y deduplicación a nivel de bloque
- Software o tecnología 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 puede regenerarse utilizando los niveles de protección solicitados.

El equipo cuenta 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.

2.1.1.2.4 UNIDAD DE RESPALDO DE PLATAFORMA ABIERTA

KIO Networks dará el servicio de respaldo de aplicaciones desarrolladas en plataforma abierta, por lo que el equipo cuenta con las siguientes características:

- Contar con una capacidad base usable de almacenamiento de al menos 90TB con protección de tipo mínimo RAID 6
- 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 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 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.

El equipo permite la recuperación mediante snaps y clones
El equipo incluye todo el licenciamiento de software requerido para cumplir con los requerimientos.
En caso de falla de algún componente del equipo utilizado por **KIO Networks**, el contenido almacenado podrá regenerarse utilizando los niveles de protección solicitados.
El equipo cuenta 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 6.

2.1.1.2.5 UNIDAD DE RESPALDO DE CINTAS

- **KIO Networks** provee la infraestructura para la realización de respaldos y restauraciones de información. **KIO Networks** incluye el hardware, software y soporte para realizar los respaldos y restauraciones.
- La librería no tiene anuncio de fin de vida y cuenta con al menos las capacidades solicitadas.
- La librería será dedicada y de uso exclusivo para el Instituto.
- Como parte de la infraestructura se deberá contemplar al menos un servidor para la consola de respaldos en plataforma UNIX , LINUX o WINDOWS, que realice respaldos a disco, cinta virtual o cinta física, así como el manejo de librerías físicas y virtuales.
- La solución de respaldos deberá enviar la información a disco y posteriormente a cinta, para ello se ocuparán los BCFs correspondientes y de acuerdo con la vigencia y/o uso de la información, estas pasarán a respaldarse en cinta como información histórica.
- **KIO Networks** en conjunto con el Instituto acordará las políticas de respaldo y retención, las cuales podrán ser actualizadas de común acuerdo con **KIO Networks**, para una mejor operación.
- La solución propuesta cuenta con la capacidad de deduplicación y utilizar la última y/o penúltima versión liberada, de la herramienta de respaldos.
- La solución de respaldos deberá tener la capacidad de realizar respaldos totales, incrementales, diferenciales y/o consolidados.
- Deberá contar con un monitoreo, donde se pueda ver el estatus de los respaldos y generar notificaciones automáticas de respaldos fallidos, por ejemplo, vía correo electrónico, preferentemente deberá integrarse con la herramienta de Monitoreo propuesta.
- La solución de respaldos deberá permitir navegar por los objetos respaldados (archivos y directorios) y a partir de ahí, seleccionar la información que se desea recuperar, la información a restaurar deberá ser mostrada de forma similar a la de un explorador de Windows, permitiendo la navegación por los diferentes niveles de los objetos a restaurar.

ANEXOS
DIVISIÓN DE CONTRATOS

- La solución de respaldos deberá permitir ejecutar respaldos y recuperaciones de manera calendarizada, para verificar la integridad física y lógica de los respaldos con el objeto de asegurar que los datos fueron correctamente grabados.
- La solución de respaldos deberá permitir asignar distintas políticas de retención, las cuales dependen del tipo de información, el medio de almacenamiento y la fecha de realización del respaldo, cuando se requiera tener una expiración indefinida para un respaldo, se debe permitir el manejo de archivado y su restauración al ser requerido.
- La solución de respaldos deberá permitir la restauración de información en servidores diferentes al origen del respaldo.
- La solución de respaldos ofertada deberá soportar la integración con soluciones de virtualización.
- Deberá proporcionar la plataforma respaldos en Cintas para el Centro de Datos Principal y deberá contar con al menos las siguientes características técnicas.
    - 4 Drives LTO8 con un total de 100 slots
    - Contar con un sistema de respaldo en cinta al menos LTO-8.
    - Las cintas LTO-8 necesarias para mantener la operación durante la vigencia del contrato, serán solicitadas en su BCF correspondiente.
    - Deberá proporcionar el licenciamiento necesario para encriptación y administración, sin costo para el Instituto.

Las cintas serán resguardadas como parte del servicio entregado por **KIO Networks** y el precio unitario ofertado para ejercer su resguardo estará asociado a paquetes de 50 cintas por unidad.

2.1.1.2.6 UNIDAD DE ALMACENAMIENTO DE DATOS DE ALTO RENDIMIENTO Y RED SAN

KIO Networks dará el servicio de almacenamiento de Datos de alto rendimiento y red SAN, por lo que el equipo cuenta con las siguientes características:

- 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)
- Permitir la configuración de por lo menos los siguientes RAID:
    - .
    - RAID 5: (3 + 1) o (7 +1) para todas las unidades.
- Ser compatible con la plataforma Mainframe.

El equipo tiene 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 incluye 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 permite la continuidad de la operación en caso de cualquier contingencia.
En caso de falla de algún componente del equipo utilizado por **KIO Networks**, el contenido almacenado podrá regenerarse utilizando los niveles de protección solicitados.

El equipo cuenta 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 o superior.

2.1.1.3 MODULO DE ALMACENAMIENTO EXTRAIBLES

2.1.1.3.1 UNIDAD INDIVIDUAL DE RESPALDOS (PORTATIL)

KIO Networks dará el servicio de un equipo de unidad de respaldos portátil, el cual tendrá 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:

ANEXOS
DIVISIÓN DE CONTRATOS

  - 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

2.1.2.1 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. **KIO Networks** ejecutará las acciones necesarias para garantizar la continuidad de la operación.

Requerimientos Mínimos

Para este servicio se considerarán los componentes de infraestructura 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 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. **KIO Networks** ejecutará 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

2.1.2.1.3 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. **KIO Networks** ejecutará las acciones necesarias para garantizar la continuidad de la operación en esta plataforma.

Requerimientos Mínimos:

- Hacer uso de la subscripción de soporte de ORACLE SERVER LINUX (6 o superior) o equivalente (soporte empresarial 7/24 en línea y presencial a través del contrato de licenciamiento y soporte que tiene contratado el Instituto con el fabricante, 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 a través del contrato de soporte y licenciamiento con el que cuenta el Instituto con Oracle
- Atención y solución de incidentes de forma proactiva
- Análisis de comportamiento y plan de previsión

2.1.3 Plataformas de Virtualización

2.1.3.1 SERVIDORES

2.1.3.1.1 SERVIDOR VIRTUAL RISC MODALIDAD CDP, ENP Y SDI

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
  - 8 threads por procesador

Y deberá ser escalable con al menos incrementos de:

- Módulos de 1 core con 8 threads por core

La memora RAM BASE deberá ser cuando menos de:

ANEXOS
DIVISIÓN DE CONTRATOS

- 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 **KIO Networks** establece un incremento de 1GB de memoria que oferta **KIO Networks**.

La Interface de red deberá incluir por lo menos:
- 5puertos 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 cuenta con tarjeta de administración remota que permite la administración del mismo en una interfaz de modo texto, incluso si el equipo está apagado.

El Sistema Operativo es 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 *

* Más actualización de parches

2.1.3.1.2 SERVIDOR VIRTUAL X86 MODALIDADES CDP, ENP Y SDI

El Procesador será 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 de procesador físico
  - Capacidad base de 4 vCPUs de procesador virtual

Y deberá ser escalable con al menos incrementos de:
- Módulos de 4 vCPUs

La memora RAM BASE deberá ser cuando menos de:

- 16 GB de memoria RAM

Incremento de 8 GB de memoria RAM Servidores virtuales 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 **KIO Networks** establece un incremento de 8 GB de memoria que oferta **KIO Networks**.

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

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.

El equipo cuenta 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 es compatible, entre otras, con las siguientes versiones de Sistema Operativo:

- Oracle Linux 5X, 6X o 7X
- Windows 2012 / 2014 Server o superior
- Diferentes Distribuciones Linux

ANEXOS
DIVISIÓN DE CONTRATOS

2.1.3.2 ENTORNO PARA EL USUARIO FINAL

2.1.3.2.1 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
- Puerto de red Ethernet
- 6 Puertos USB
- Mouse óptico de 2 botones
- Teclado en español
- Monitor de 19 pulgadas como mínimo

2.1.3.2.2 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

2.1.4.1 PLATAFORMA DE VIRTUALIZACIÓN

2.1.4.1.1 PLATAFORMA DE VIRTUALIZACIÓN MULTI-TECNOLOGIA

KIO Networks suministrará una plataforma de virtualización que soporte las diferentes tecnologías de sistema operativo, las cuales deberán dar continuidad a las que hoy en día tiene el Instituto en operación: VMWare, OVM y KVM

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, con capacidad de soportar hasta 800 cores por Plataforma.

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 **KIO Networks** 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. Las nuevas deberán soportar los últimos sistemas operativos liberados por el fabricante del mismo.

- 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, cuando sea requerido por el Instituto y 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.

2.2 Red

2.2.1 Zona

2.2.1.1 PUNTO NEUTRO

El Instituto requiere establecer comunicación desde diferentes ubicaciones o localidades remotas hacia el centro de datos ofertado por **KIO Networks**, donde podrán converger 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 través del cual se brindarán accesos a internet, para la consulta y transferencia de información, así como se hará la publicación de servicios WEB.

ANEXOS
DIVISIÓN DE CONTRATOS

Características mínimas a cumplir en cuanto a capacidad, funcionalidad, operación y disponibilidad del punto neutro:

- Deberá incluir Interfaces Físicas 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.
  - Flexibilidad de manejo de tráfico con la configuración de clases de servicio sobre el tráfico de WAN público y WAN privado.
  - 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 al menos 100 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 al menos 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:

- 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 proporcionarse 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 proporcionarse en alta disponibilidad.
- 1 Enlace MPLS redundante 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 proporcionarse en alta disponibilidad.

El Punto Neutro debe incluir las siguientes características, funcionalidades y servicios.

2.2.1.1.1 RED DE AREA AMPLIA (WAN)

Para Punto Neutro la Red de Área 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 incluye 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 tráfico 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 críticas.
- 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.

2.2.1.1.2 RED DE AREA 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), redireccionándolos hacia los destinos correspondientes.

El Servicio de Red de Área Local en el Centro de Datos ofertado por **KIO Networks** considera e incluye 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.

ANEXOS
DIVISIÓN DE CONTRATOS

El Servicio considera e incluye toda la infraestructura y los insumos necesarios para brindar conectividad a las diferentes aplicaciones del Instituto y dispositivos de TICS que así lo requieran.
Cuenta con mecanismos de separación de tráfico para coadyuvar a una mejor administración de la infraestructura de TICS.

Mantiene 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:

- **KIO Networks** creará 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.
- **KIO Networks** garantizará 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 **KIO Networks** considera el equipamiento necesario para lograrlo.
- **KIO Networks** 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 esta permitido que paquetes de datos de otros clientes de **KIO Networks** viajen a través de las VLAN's que se implementen para el Instituto.
- El incumplimiento del aislamiento de las VLAN's por parte de **KIO Networks**, se interpretará como un incumplimiento del servicio y una violación del acuerdo de confidencialidad que se solicita a **KIO Networks** por lo que éste se hará acreedor a las sanciones correspondientes.
- **KIO Networks** considera e incluye 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 podrán ser solicitados a través del consumo de los BCFs correspondientes, pues se entiende que forman parte de la arquitectura integral del servicio solicitado por el 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 de **KIO Networks**, con la finalidad de verificar el cumplimiento de lo solicitado.
- **KIO Networks** considera e incluye 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.
- **KIO Networks** integrará todo lo necesario para soportar la recepción de enlaces LAN to LAN (L2L), para generar la conectividad con terceros.

2.2.1.1.3 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, redireccionándolos hacia los destinos correspondientes.

KIO Networks considera e incluye 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.

Cuenta con 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 considera e integran 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 y notificación de Red y Abusos mediante un Noc y SOC respectivamente a través del proceso de Gestión de Eventos.
- 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.
- Capacidad de integrar 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.

Cuenta con el Monitoreo y seguimiento del direccionamiento homologado del IMSS necesarios para la entrega de los servicios descritos en el presente Anexo Técnico.
Se generarán reportes de capacidad de infraestructura de datos para el crecimiento con las menores afectaciones a la operación.

2.2.1.1.4 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, redireccionándolos hacia los destinos correspondientes.

KIO Networks considera e incluye toda la infraestructura y los insumos necesarios para brindar conectividad a las diferentes aplicaciones del Instituto y dispositivos de TICS que así lo requieran.

ANEXOS
DIVISIÓN DE CONTRATOS

KIO Networks mantendrá 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 de **KIO Networks**, 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.
- **KIO Networks** considera e incluye 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.
- 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 de **KIO Networks**, con la finalidad de verificar el cumplimiento de lo solicitado.

2.2.1.1.5 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 establecerá comunicación hacia un Portal Institucional desde diferentes ubicaciones o localidades remotas hacia el centro de datos ofertado por **KIO Networks**, 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 cuenta 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.

2.2.2 Pública

2.2.2.1 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 a **KIO Networks** para brindar el servicio. Esta calidad de servicio se alcanza implementando mecanismos de control de retardo y prioridad de tráfico que aseguran técnicamente y operativamente un trato homogéneo para las aplicaciones en todo el trayecto de los flujos.

Considera la integración de una solución que identifica 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. **KIO Networks** 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 podrá darse a través de 2 tipos de enlaces

2.2.2.1.1 ENLACE MPLS

KIO Networks brindará 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.

ANEXOS
DIVISIÓN DE CONTRATOS

- 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.
- **KIO Networks** cuenta con los medios que le permiten 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 incluye 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.

2.2.2.1.2 ENLACES LAN TO LAN

KIO Networks 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% aplicable sobre la falla de ambos enlaces.
- Infraestructura dedicada.
- El apego a las políticas de acceso físicas al Punto Neutro, serán las estipuladas por **KIO Networks** en acuerdo con el Instituto.

- El centro de operaciones de 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 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 incluye 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.

2.2.3 Infraestructura de Red

2.2.3.1 VIRTUALIZACION DE REDES

2.2.3.1.1 BALANCEADOR DE CARGA DE CAPAS L4-L7

KIO Networks dará el suministro de servicios de Balanceo L4-L7 para aplicaciones Web o equivalente y su información inherente. La infraestructura propuesta cumple 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

ANEXOS
DIVISIÓN DE CONTRATOS

2.3 Instalaciones

2.3.1 Co-ubicación en modalidades de despliegue

2.3.1.1 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 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.

2.3.1.2 MODALIDADES DE CO-UBICACIÓN

2.3.1.2.1 PISO BLANCO

KIO Networks dará el servicio de metro cuadrado de piso blanco en las instalaciones de **KIO Networks**, con la finalidad de poder alojar equipamiento propio o de otros proveedores externos en las instalaciones de **KIO Networks** y para lo cual cuenta 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.

2.3.1.2.2 ESPACIO EN RACK

KIO Networks dará el servicio de unidades de espacio en Rack en las instalaciones de **KIO Networks**, con la finalidad de poder alojar equipamiento propio o de otros proveedores externos en las instalaciones de **KIO Networks** y para lo cual cuenta 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 de **KIO Networks** 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 Análisis estadístico

3.1.1 Sistema de Gestión de bases de datos

3.1.1.4 SUSCRIPCION DE BASES DE DATOS OPEN SOURCE

El Instituto podrá solicitar a **KIO Networks** 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, **KIO Networks** realizará 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 como:
  - Stanalone
  - Cluster (HA)

- **KIO Networks** considerará al menos las siguientes plataformas de Base de Datos opencource: PostgreSQL, MySQL, Maria DB, Berkeley DB (con licencia GNU AGPL), Cassandra DB, Mongo DB y Hadoop.
- 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.
- Arrancar o levantar la base de datos en modo normal después de haberla diseñado.
- Crear y otorgar privilegios a usuarios y roles en la base de datos.

ANEXOS
DIVISIÓN DE CONTRATOS

- 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 OpenSource 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 disponibles como parches provisionales individuales y como conjuntos de parches.

3.2 Herramientas y entorno de desarrollo

3.2.1 Entorno de desarrollo integrado (IDE)

3.2.1.1 KIT DE DESARROLLO DE SOFTWARE (SDK)

3.2.1.1.1 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. **KIO Networks** ejecutará las acciones necesarias para garantizar la continuidad de la operación haciendo uso del acuerdo de Licenciamiento y soporte suscrito entre el Instituto y el fabricante.

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

3.2.2 Gestión de documentos y contenidos

3.2.2.1 GESTIÓN DE CONTENIDOS WEB

3.2.2.1.1 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. **KIO Networks** ejecutará 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

3.2.2.1.2 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.

KIO Networks ejecutará 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

3.2.2.1.3 ALFRESCO

El Instituto requiere de servicios de para gestión de contenido Alfresco a través de una plataforma integrada que brinde servicios, repositorios, API, soluciones y herramientas de procesamiento empresarial centrados en el contenido para promover la transformación digital. La plataforma Alfresco debe contar con las siguientes funcionalidades:

- gestión de documentos,
- procesos de back-office,
- aplicaciones de procesos de negocio,
- gestión de registros
- productividad del equipo.

La plataforma de gestión de contenido debe permitir la creación de un repositorio propio. Los servicios y datos deberán integrarse con aplicaciones y repositorios externos no nativos a través de conectores prediseñados, desarrollo de API o integraciones.

La plataforma debe ofrecer interfaz de aplicaciones web que permita a los usuarios navegar y trabajar con los diferentes servicios de contenido. La plataforma debe ofrecer soluciones prediseñadas para procesos de contenido verticales y horizontales.

El licenciamiento será por core o por nodo de acuerdo al esquema definido por el fabricante.

3.3 Middleware

3.3.1 Bus de servicios empresariales (ESB)

3.3.1.1 SOFTWARE DE MENSAJERIA

3.3.1.1.1 TUXEDO

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma TUXEDO o equivalente según sus necesidades. **KIO Networks** ejecutará las acciones necesarias para garantizar la continuidad de la operación.

ANEXOS
DIVISIÓN DE CONTRATOS

Requerimientos Mínimos:

- Software de TUXEDO Support o equivalente (soporte empresarial que incluye Indemnización legal), haciendo uso del Licenciamiento y soporte provisto por el Instituto.
- Versión del producto 9.2 y posteriores
- Soporte del producto por 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

3.3.1.1.2 GLASSFISH

El Instituto podrá solicitar durante la vigencia del contrato los servicios de administración de la plataforma GLASSFISH o equivalente según sus necesidades. **KIO Networks** ejecutará 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

3.3.1.1.3 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. **KIO Networks** ejecutará 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

3.3.1.1.4 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. **KIO Networks** ejecutará 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

3.4 Comunicación unificada y colaboración

3.4.1 Correo electrónico

3.4.1.1 SERVICIO DE CORREO ELECTRÓNICO

Se requiere el servicio de la administración del correo electrónico corporativo durante la vigencia del contrato. Los requisitos mínimos que **KIO Networks** considera 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:

Perfil de Usuarios	Cuota de Buzón en MB	% de Usuarios por perfil
Operativos	10	80
Operativos	20	5
Operativos	50	5

ANEXOS
DIVISIÓN DE CONTRATOS

Perfil de Usuarios	Cuota de Buzón en MB	% de Usuarios por perfil
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.

Respaldos, Restauración y Depuración de la Información

El Proveedor deberá establecer un esquema de respaldos en línea, restauración y depuración 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, los mensuales de 3 meses,y el anual 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

Protección en el correo electrónico

- 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

- **KIO Networks** garantiza la confidencialidad de la información vinculada al resguardo y almacenamiento de las cuentas de correo electrónico.

4 OPERACIÓN DIGITAL

4.1 Servicios Generales

4.1.1 Gestión de la seguridad cibernética

4.1.1.1 IDENTIFICACION Y AUTENTICACIÓN

4.1.1.1.1 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

ANEXOS
DIVISIÓN DE CONTRATOS

4.1.2 Soporte para la entrega de servicios institucionales

4.1.2.1 INFRAESTRUCTURA WEB

4.1.2.1.1 SOLUCION PARA EL CUMPLIMIENTO WCAG

Los Web Content Accessibility Guidelines (Directrices de Accesibilidad para el Contenido Web, WCAG por sus siglas en inglés) son una parte de las directrices de accesibilidad web publicados por la Web Accessibility Initiative (Iniciativa de Accesibilidad Web, WAI) parte del World Wide Web Consortium (W3C), la principal organización de estándares de internet.

Son un conjunto de directrices que especifican cómo hacer el contenido web más accesible, especialmente a personas con discapacidades. La versión actual de estas directrices es la WCAG 2.0, publicado en diciembre de 2008 y convertido en estándar ISO/IEC 40500:2012 en octubre de 2012.

KIO Networks dará el servicio de Solución para el cumplimiento WCAG durante la vigencia del contrato con las siguientes características:

- Plataforma que se pueda integrar al Portal Web del Instituto con una instalación tipo “one-line-code”.
- Que cumpla con los estándares: WCAG 2.0, WCAG 2.1, ADA, Section 508.
- Lector de pantalla.
- Navegación por teclado.
- Bloqueo de parpadeo.
- Manejo de contraste y de colores.
- Manejo de tamaño de fuente.

3 FIRMAS DE ELABORACION, REVISION Y APROBACION

Atentamente

DocuSigned by:
413DA358D32D4B3...

JUAN CARLOS MARTÍNEZ VALDÉS
REPRESENTANTE LEGAL
SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.

KIO Networks

DS JCMV DS JAR

DocuSign Envelope ID: 658B6DB9-3AF3-424C-8656-941FE346D1BF

Apéndice 2

Ubicaciones Geográficas

SGMP_Apéndice_2

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

Ciudad de México a 13 de abril de 2022

Esta información es propiedad de Sixsigma Networks México, S.A. de C.V. (KIO NETWORKS), se proporciona con el carácter de confidencial. Esta información no será reproducida, usada o divulgada total o parcialmente por cualquier razón diferente que la de evaluar la propuesta de Servicios de KIO NETWORKS.

ANEXOS
DIVISIÓN DE CONTRATOS

ÍNDICE

1 OBJETIVO DEL DOCUMENTO 3
2 CONSIDERACIONES GEOGRAFICASDE CENTRO DE DATOS PRIMARIO 3
3 UBICACIONES INICIALES DE EXTENSION DE NUBE PRIVADA 3
4 FIRMAS DE ELABORACION, REVISION Y APROBACION 7

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.

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 GEOGRAFICASDE CENTRO DE DATOS PRIMARIO

Éste deberá estar ubicado en territorio nacional.

3 UBICACIONES INICIALES DE EXTENSION 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.

De manera enunciativa mas no limitativa, 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.

KIO Networks®

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

- 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.

- DELEGACIÓN CDMX NORTE - LA RAZA (5)
  - HE CMN La Raza: Calle Seris No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Ciudad de México.
  - HGO 3 CMN La Raza: Avenida Vallejo esq Antonio Valeriano No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Ciudad de México.
  - HI CMN La Raza: Circuito Interior Paseo de las Jacarandas No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Ciudad de México.
  - HG CMN La Raza: Circuito Interior Paseo de las Jacarandas No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Ciudad de México.
  - BS CMN La Raza: Calle Seris No. S/N, Colonia La Raza C.P. 02990 Azcapotzalco, Delegación Azcapotzalco, Ciudad de México.

- DELEGACIÓN CDMX 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, Ciudad de México
  - 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, Ciudad de México

- DELEGACIÓN CDMX SUR - SXXI (5)
  - HE CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Ciudad de México.
  - HP CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Ciudad de México.
  - HC CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Ciudad de México.
  - HONCO CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Ciudad de México.
  - BS CMN Siglo XXI: Avenida Cuauhtémoc No. 330, Colonia Doctores C.P. 6720 Cuauhtémoc, Delegación Cuauhtémoc, Ciudad de México.

- DELEGACIÓN CDMX SUR - SAN ANGEL (2)
  - HGO 4 CMN Siglo XXI San Ángel Eje Vial Eje 10 Sur Río Magdalena No. 289, Colonia Tizapán San Ángel C.P. 1090 Álvaro Obregón, Delegación Álvaro Obregón, Ciudad de México.
  - HGZMF 8 San Ángel: Avenida Río Magdalena No. 289, Colonia Tizapán San Ángel C.P. 1090 Álvaro Obregón, Delegación Álvaro Obregón, Ciudad de México.

- 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.

ANEXOS
DIVISIÓN DE CONTRATOS

- 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:

- 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

DS JCHV DS JAR

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 ELABORACION, REVISION Y APROBACION

Atentamente

DocuSigned by:
413DA358D32D4B3...

JUAN CARLOS MARTÍNEZ VALDÉS
REPRESENTANTE LEGAL
SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.

KIO Networks

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

DocuSign Envelope ID: 658B6DB9-3AF3-424C-8656-941FE346D1BF

Apéndice 3

Esfuerzos realizados para la migración de Centro de Datos Actual

SGMP_Apéndice_3

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

Ciudad de México a 13 de abril de 2022

Esta información es propiedad de Sixsigma Networks México, S.A. de C.V. (KIO NETWORKS), se proporciona con el carácter de confidencial. Esta información no será reproducida, usada o divulgada total o parcialmente por cualquier razón diferente que la de evaluar la propuesta de Servicios de KIO NETWORKS.

ANEXOS
DIVISIÓN DE CONTRATOS

ÍNDICE

1 OBJETIVO DEL DOCUMENTO 3
2 TIPOS DE APLICACIONES INSTITUCIONALES 3
3 COMPLEJIDAD DE LAS APLICACIONES 3
4 RECURSOS HUMANOS 4
5 CALENDARIOS DE MIGRACION 4
6 TABLA DE ESFUERZO DE MIGRACION 4
7 APLICACIONES MIGRADAS 6
8 FIRMAS DE ELABORACION, REVISION Y APROBACION 16

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.

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.

KIO Networks®

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

- 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 MIGRACION

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 MIGRACION

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				

KIO Networks

DS JCHV DS JAR

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 Administración 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		

KIO Networks

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

SHAREPOINT y TFS	Fuerza de Trabajo	Oracle	Microsoft	IMSS	Total
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
5	Administración de Usuarios de los Servicios Digitales	DIR	Implementado inicialmente en	Mediano	

DS JCHV DS JAR

			centro de datos externo		
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

KIO Networks®

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

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 externo	Bajo	
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

ANEXOS
DIVISIÓN DE CONTRATOS

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	
69	Nuevo Sistema Monitor de Incapacidades	DPM	Migrado	Bajo	300

KIO Networks

DS JCHV DS JAR

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

ANEXOS
DIVISIÓN DE CONTRATOS

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	

KIO Networks

DS JCHV DS JAR

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

ANEXOS
DIVISIÓN DE CONTRATOS

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 Internet	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 externo	Mediano	
145	Micrositio Estar Bien Capacitación Virtual	DG	Implementado inicialmente en centro de datos externo	Bajo	

KIO Networks

DS JCHV DS JAR

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 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 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

ANEXOS
DIVISIÓN DE CONTRATOS

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 ELABORACION, REVISION Y APROBACION

Atentamente

DocuSigned by:
413DA358D32D4B3...

JUAN CARLOS MARTÍNEZ VALDÉS
REPRESENTANTE LEGAL
SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.

KIO Networks

DS JCHV DS JAR

DocuSign Envelope ID: 658B6DB9-3AF3-424C-8656-941FE346D1BF

Apéndice 4

Relación actual de Infraestructura en Centro de Datos y proyección de crecimiento

SGMP_Apéndice_4

Coordinación de Servicios de Infraestructura Tecnológica Institucional

KIO Networks

Servicio de Continuidad de Nube IMSS 2022

Ciudad de México a 13 de abril de 2022

Esta información es propiedad de Sixsigma Networks México, S.A. de C.V. (KIO NETWORKS), se proporciona con el carácter de confidencial. Esta información no será reproducida, usada o divulgada total o parcialmente por cualquier razón diferente que la de evaluar la propuesta de Servicios de KIO NETWORKS.

ANEXOS
DIVISIÓN DE CONTRATOS

ÍNDICE

1 OBJETIVO DEL DOCUMENTO 3
2 RELACION ACTUAL DE INFRAESTRUCTURA 3
3 DESCRIPCION DE CONCEPTOS SEGÚN SERVICIO ACTUAL DEL CENTRO DE DATOS 5
3.1 Servidor X86 5
3.2 Módulo de Seguridad en Hardware (HSM) 5
3.3 Almacenamiento de Datos Individual 6
3.4 Respaldo de Datos Individual 6
3.5 Unidad de almacenamiento de media categoría para aplicaciones de bajo desempeño 6
3.6 Unidad de respaldo de plataforma abierta 7
3.7 Unidad de Almacenamiento de Datos de alto rendimiento y red SAN 7
3.8 Unidad individual de respaldos (Portatil) 7
3.9 Sistema Operativo Red Hat Enterprise Linux 8
3.10 Sistema Operativo SLES 8
3.11 Sistema Operativo Windows Server 2008 8
3.12 Sistema Operativo Windows 2012 8
3.13 Servidor Virtual RISC SPARC 9
3.14 Servidor Virtual X86 4VCPU 16 RAM 9
3.15 Puntos de Acceso a la Nube 9
3.16 Escritorio en la Nube 9
3.17 Plataforma de Virtualización multi-tecnología 10
3.18 Punto Neutro 10
3.19 Enlaces para conectividad de Red de Área Amplia e Internet 10
3.20 Balanceador de carga de capas L4-L7 11
3.21 Plataforma Nodo de Extensión de Nube Privada - Tamaño grande 11
3.22 Piso Blanco 11
3.23 Espacio en Rack 11
3.24 Oracle 11
3.25 Microsoft SQL Server 12
3.26 Subscripciones a Bases de Datos Open Source 12
3.27 Liferay Enterprise 12
3.28 GlassFish 13
3.29 Apache Tomcat 13
3.30 Apache HTTPD 13
3.31 Servicio de correo electrónico 13
3.32 Firewall 13
3.33 IPS 13
3.34 Anti-Denegación de Servicios (DDoS) 14
3.35 Redes Privadas Virtuales – VPN 14
3.36 Gestión Unificada de Amenazas (UTM) 14
3.37 Firewall Especializado en Servicios Web (WAF) 14
3.38 Nodo de red con UTP 15
3.39 Nodo de red con Fibra óptica 15
3.40 Switch de 10G de core 15
3.41 Switch de 1G de distribución 15
3.42 Sistema de Almacenamiento de datos en RAID5 de 12TB con capacidad de crecimiento hasta 32TB 15
3.43 Solución para el cumplimiento WCAG 15
4 PROYECCION DE CRECIMIENTO 16
5 FIRMAS DE ELABORACION, REVISION Y APROBACION 18

KIO Networks

DS JCHV DS JAR

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.

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 2022, 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 RELACION 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.

Descripción	Cantidad	Unidad de medida
Servidor X86	689	Servicio
Incrementos de Módulos de 1 Procesador con 128 threads X86	44	Servicio
Incrementos de 128GB de memoria RAM X86	22	Servicio
Módulo de Seguridad en Hardware (HSM)	1	Servicio
Almacenamiento de Datos Individual	531	Servicio
Incremento de Almacenamiento de Datos Individual de 100GB	5079	Servicio
Respaldo de Datos Individual	81	Servicio
Unidad de almacenamiento de media categoría para aplicaciones de bajo desempeño	2	Servicio
Incremento en disco de estado sólido 1TB para almacenamiento bajo desempeño	1	Servicio
Incremento en disco FC solido 1TB usable para almacenamiento bajo desempeño (SATA)	16	Servicio
Unidad de respaldo de plataforma abierta	6	Servicio

ANEXOS
DIVISIÓN DE CONTRATOS

Descripción	Cantidad	Unidad de medida
Incremento de bloques de 30TB usables en arreglo RAID 5 para unidades de plataforma abierta	13	Servicio
Unidad de Almacenamiento de Datos de alto rendimiento y red SAN	1	Servicio
Incremento en discos de estado sólido 1TB para almacenamiento de alto rendimiento	98	Servicio
Unidad individual de respaldos (Portatil)	505	Servicio
Sistema Operativo Red Hat Enterprise Linux	35	Servicio
Sistema Operativo SLES	11	Servicio
Sistema Operativo Oracle Linux Server	0	Servicio
Sistema Operativo Windows Server 2008	0	Servicio
Sistema Operativo Windows 2012	0	Servicio
Servidor Virtual RISC SPARC	16	Servicio
Incremento de 1 Procesador Virtual con 128 threads RISC	11	Servicio
Incremento de 32GB de memoria Virtual RAM RISC	6	Servicio
Servidor Virtual X86 4VCPU 16 RAM	510	Servicio
Incremento Virtualizado Módulos de 1 Procesador Virtual con 8 threads X86	436	Servicio
Incremento Virtualizado 8GB de memoria RAM X86	521	Servicio
Puntos de Acceso a la Nube	1322	Servicio
Escritorio en la Nube	955	Servicio
Plataforma de Virtualización multi-tecnologia	2	Servicio
Punto Neutro	1	Servicio
Conectividad de Enlaces MPLS 5 Gbps redundante activo – activo	3	Servicio
Conectividad de Enlaces Lan2Lan 100 Mbps redundante activo – activo	1	Servicio
UTM para enlaces de banda ancha hasta 100 Mbps	1	Servicio
UTM para enlaces de banda ancha hasta 10 Gbps	2	Servicio
Balanceador de carga de capas L4-L7	3	Servicio
Plataforma Nodo de Extensión de Nube Privada - Tamaño grande	1	Servicio
Piso Blanco	3	Servicio
Espacio en Rack	1	Servicio
Tableau Server	0	Servicio
Tableau Desktop	0	Servicio
Bases de Datos Oracle – StandAlone	0	Servicio
Bases de Datos Oracle – RAC	0	Servicio
Microsoft SQL Server	0	Servicio
Subscripciones a Bases de Datos Open Source	1	Servicio
Java Development Kit	3	Servicio
Liferay Enterprise 7/24	8	Servicio
Liferay Enterprise 5/8	0	Servicio
Alfresco	4	Servicio
WebLogic	0	Servicio
GlassFish	8	Servicio
Apache Tomcat	1	Servicio
Apache HTTPD	97	Servicio
Servicio de correo electrónico.	92051	Servicio
Firewall	6	Servicio
IPS	2	Servicio

KIO Networks

DS JCHV DS JAR

Descripción	Cantidad	Unidad de medida
Anti-Denegación de Servicios (DDoS)	2	Servicio
Redes Privadas Virtuales – VPN	2	Servicio
Gestión Unificada de Amenazas (UTM)	4	Servicio
Firewall Especializado en Servicios Web (WAF)	2	Servicio
Nodo de red con UTP	629	Servicio
Nodo de red con Fibra óptica	64	Servicio
Switch de 10G de core	16	Servicio
Switch de 1G de distribución	70	Servicio
UTM para enlaces a Red Nacional para Impulso de la Banda Ancha (NIBA) de 100 Mbps	1	Servicio
Enlaces Internet 100 Mbps redundante activo – activo	4	Servicio
Sistema de Almacenamiento de datos en RAID5 de 12TB con capacidad de crecimiento hasta 32TB	74	Servicio
Solución para el cumplimiento WCAG	1	Servicio

La información expresada es de carácter informativo y no representa un compromiso del Instituto respecto al comportamiento de los servicios, ya que los mismos son bajo demanda conforme a las necesidades del Instituto.

3 DESCRIPCION DE CONCEPTOS SEGÚN SERVICIO ACTUAL DEL 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
  - Mínimo 8 cores por procesador

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

ANEXOS
DIVISIÓN DE CONTRATOS

- 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

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

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.

ANEXOS
DIVISIÓN DE CONTRATOS

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

ANEXOS
DIVISIÓN DE CONTRATOS

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 Virtualización multi-tecnología

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 autocontenido 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

AUTOS
DIVISIÓN DE CONTRATOS

- GlassFish
- Oracle ODI
- Sistema Operativo Oracle Linux Server
- WebLogic

3.25 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.

3.26 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.

3.27 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

3.28 GlassFish

Administración de la plataforma GLASSFISH o equivalente según sean sus necesidades. Incluye las acciones necesarias para garantizar la continuidad de la operación.

3.29 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.

3.30 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.

3.31 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.

3.32 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.

3.33 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 previene fugas de información.

ANEXOS
DIVISIÓN DE CONTRATOS

3.34 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.

3.35 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).

3.36 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

Los servicios de Antimalware y Filtrado de Contenido Web forman parte de los módulos del UTM integrados dentro del mismo dispositivo. Referente al Antispam, este no formara parte de los módulos del mismo, y el Instituto suministrara el software como parte de los contratos actuales que cuenta con terceros.

3.37 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.

3.38 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.

3.39 Nodo de red con Fibra óptica

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.

3.40 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

3.41 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.

3.42 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.

3.43 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.

ANEXOS
DIVISIÓN DE CONTRATOS

4 PROYECCION DE CRECIMIENTO

Descripción	2020	2021
Servidor X86	689	
Incrementos de Módulos de 1 Procesador con 128 threads X86	44	
Incrementos de 128GB de memoria RAM X86	22	
Módulo de Seguridad en Hardware (HSM)	1	
Almacenamiento de Datos Individual	531	
Incremento de Almacenamiento de Datos Individual de 100GB	5079	
Respaldo de Datos Individual	81	
Unidad de almacenamiento de media categoría para aplicaciones de bajo desempeño	2	
Incremento en disco de estado sólido 1TB para almacenamiento bajo desempeño	1	
Incremento en disco FC solido 1TB usable para almacenamiento bajo desempeño (SATA)	16	
Unidad de respaldo de plataforma abierta	6	
Incremento de bloques de 30TB usables en arreglo RAID 5 para unidades de plataforma abierta	13	
Unidad de Almacenamiento de Datos de alto rendimiento y red SAN	1	
Incremento en discos de estado sólido 1TB para almacenamiento de alto rendimiento	98	
Unidad individual de respaldos (Portatil)	505	
Sistema Operativo Red Hat Enterprise Linux	35	
Sistema Operativo SLES	11	
Sistema Operativo Oracle Linux Server	0	
Sistema Operativo Windows Server 2008	0	
Sistema Operativo Windows 2012	0	
Servidor Virtual RISC SPARC	16	
Incremento de 1 Procesador Virtual con 128 threads RISC	11	
Servidor Virtual X86 4VCPU 16 RAM	6	
Incremento Virtualizado Módulos de 1 Procesador Virtual con 8 threads X86	510	
Incremento Virtualizado 8GB de memoria RAM X86	436	
Puntos de Acceso a la Nube	521	
Escritorio en la Nube	1322	
Plataforma de Virtualización multi-tecnología	955	
Punto Neutro	2	
Conectividad de Enlaces MPLS 5 Gbps redundante activo - activo	1	
Conectividad de Enlaces Lan2Lan 100 Mbps redundante activo - activo	3	
UTM para enlaces de banda ancha hasta 100 Mbps	1	
UTM para enlaces de banda ancha hasta 10 Gbps	1	
Balanceador de carga de capas L4-L7	2	
Plataforma Nodo de Extensión de Nube Privada - Tamaño grande	3	
Piso Blanco	1	

KIO Networks

DS JCHV DS JAR

Descripción	2020	2021
Espacio en Rack	3	
Tableau Server	1	
Tableau Desktop	0	
Bases de Datos Oracle – StandAlone	0	
Bases de Datos Oracle – RAC	0	
Microsoft SQL Server	0	
Subscripciones a Bases de Datos Open Source	0	
Liferay Enterprise 7/24	1	
Liferay Enterprise 5/8	3	
WebLogic	8	
GlassFish	0	
Apache Tomcat	4	
Apache HTTPD	0	
Servicio de correo electrónico.	8	
Firewall	1	
IPS	97	
Anti-Denegación de Servicios (DDoS)	92051	
Redes Privadas Virtuales - VPN		
Gestión Unificada de Amenazas (UTM)		
Filtrado de Contenido Web		
Antispam		
Antimalware		
Firewall Especializado en Servicios Web (WAF)		
Nodo de red con UTP		
Nodo de red con Fibra óptica		
Switch de 10G de core		
Switch de 1G de distribución	629	
UTM para enlaces a Red Nacional para Impulso de la Banda Ancha (NIBA) de 100 Mbps	64	
Enlaces Internet 100 Mbps redundante activo - activo	16	
Sistema de Almacenamiento de datos en RAID5 de 12TB con capacidad de crecimiento hasta 32TB	70	
Solución para el cumplimiento WCAG		

ANEXOS
DIVISIÓN DE CONTRATOS

5 FIRMAS DE ELABORACION, REVISION Y APROBACION

Atentamente

DocuSigned by:
413DA358D32D4B3...

JUAN CARLOS MARTÍNEZ VALDÉS
REPRESENTANTE LEGAL
SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.

KIO Networks

DS JCHV DS JAR

DocuSign Envelope ID: 658B6DB9-3AF3-424C-8656-941FE346D1BF

Apéndice 5

Especificaciones Técnicas de Seguridad de la Información

SGMP_Apéndice_5

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

Ciudad de México a 13 de abril de 2022

Esta información es propiedad de Sixsigma Networks México, S.A. de C.V. (KIO NETWORKS), se proporciona con el carácter de confidencial. Esta información no será reproducida, usada o divulgada total o parcialmente por cualquier razón diferente que la de evaluar la propuesta de Servicios de KIO NETWORKS.

ANEXOS
DIVISIÓN DE CONTRATOS

ÍNDICE

1 OBJETIVO DEL DOCUMENTO 3
2 ESPECIFICACIONES PARA LOS COMPONENTES DE INFRAESTRUCTURA 3
2.1 FIREWALL 3
2.2 IPS 5
2.3 ANTI-DENEGACION DE SERVICIOS (DDoS) 6
2.4 GESTION UNIFICADA DE AMENAZAS (UTM) 7
2.5 FIREWALL ESPECIALIZADO EN SERVICIOS WEB (WAF) 9
2.6 CENTRO DE OPERACIONES DE SEGURIDAD (SOC) 11
3 FIRMAS DE ELABORACION, REVISION Y APROBACION 12

KIO Networks

DS JCHV DS JAR

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.

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 COMPONENTES DE INFRAESTRUCTURA

2.1 FIREWALL

Firewall para Enlaces de Banda Ancha de hasta 100 Mbps

- Deberá contar al menos con un rendimiento de 20 Gbps, en su funcionalidad de firewall.
- Deberá tener al menos un rendimiento 5 Gbps en su funcionalidad de IPS
- Mínimo deberá contar con 8 puertos 100/1000 de cobre RJ45
- Mínimo deberá soportar 2 puertos de 10 Gbps de fibra
- Mínimo deberá contar con 32 GB de memoria Desempeño de al menos 30 mil conexiones concurrentes
- Capacidad de 300k conexiones por segundo

Los Firewall deberán cumplir con al menos las siguientes funcionalidades operativas:

- Capacidad de configurar zonas, Web, App, DB, Transversales, Monitoreo, Respaldo y Operación, entre otras.
- 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.
- Deberá ser compatible con direccionamiento IPv4 e IPv6
- Deberá contar con la capacidad de manejo de al menos 1024 Vlans.

ANEXOS
DIVISIÓN DE CONTRATOS

- 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 diversas cipher suites en Secure Sockets Layer (SSL) y Transport Layer Security (TLS).
    - Deberá soportar la integración de certificados.
    - 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 v10.12, iOS desde v5, Android desde v4.2, Windows desde v10.
- Administración del sistema vía Web (HTTPS), por la línea de comando (SSH), soportar SNMPv3 y a través de una consola central de administración.
- Deberá contar con administración de políticas de al menos 500 limitado por capacidad máxima del equipo.
- Deberá contar con la capacidad de guardar histórico de cambios sobre las políticas.
- Deberá contar con doble fuente de poder que pueda ser sustituida en caliente sin afectar al dispositivo y al servicio que presta
- 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.

2.2 IPS

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

- Soporte de al menos: 20Gbps de inspección.
- Latencia máxima de 0.5 milisegundos.
- Soporte de 4 Interfaces de 10G
- Soporte Interface RJ45 para administración
- Deberá operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP.
- 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, 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 auditoría.
- 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.

ANEXOS
DIVISIÓN DE CONTRATOS

- 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

2.3 ANTI-DENEGACION DE SERVICIOS (DDoS)

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

- La solución deberá ofrecer el licenciamiento o suscripción necesario para operar en cualquiera de los ambientes sin necesidad de que la institución requiera adquirir hardware/software adicional y de manera ilimitada
- La solución deberá soportar al menos 250 Mbps.
- La solución deberá proteger al menos 2 redes IPv4 clase C con un esquema de redundancia contra ataques DDoS
- La solución deberá proporcionar los mecanismos necesarios para la mitigación de todos los tipos de ataques DDoS, ya sean basados en la Red (Capa 3, 4) o ataques de nivel aplicativo (Capa 7). Teniendo en cuenta la siguiente lista:
    - TCP SYN+ACK
    - TCP FIN
    - TCP RESET
    - TCP ACK
    - TCP ACK+PSH
    - TCP Fragment
    - UDP
    - ICMP
    - IGMP
    - HTTP Flood
    - Brute Force
    - Connection Flood
    - Slowloris
    - Spoofing
    - DNS Flood
    - Mixed SYN+UDP or ICMP+UDP Flood
    - TCP SYN+ACK
    - Ping Of Death
    - Smurf
    - Reflected ICMP and UDP
    - Teardrop
    - Zero-day DDoS attacks
- Protección contra ataques de fuerza bruta y DDoS
- Servicio de Mitigación de ataques DDoS a los aplicativos Web
- Servicio de Mitigación de ataques DDoS al servicio DNS
- Para la mitigación de ataques DDoS al servicio DNS, la plataforma de nube deberá tomar el rol de NS (NameServer), designado a través del sistema DNS global, para que sea la primera instancia que reciba

peticiones de DNS provenientes de Internet y destinadas a la infraestructura; y las reenvíe después de la inspección de seguridad.

- Deberá de tener la capacidad de definir las solicitudes de DNS válidos, en cuanto a tipo y dominio, que habrá de dejar pasar a los servidores DNS reales, bloqueando el resto de las peticiones
- Servicio de Mitigación de ataques DDoS para la Suite TCP/IP de la red pública del instituto
- Herramientas de monitoreo en tiempo real de conexiones, ancho de banda y ataques.
- Servicio de protección para API
- Servicio de prevención contra robo de cuentas de administrador
- Monitoreo y control de vulnerabilidades en las aplicaciones web críticas
- Protección avanzada contra tráfico malicioso automatizado (BOTs)
- Protección contra el uso de recursos de terceros com JavaScript en las aplicaciones Web
-
- La solución como servicio deberá garantizar un SLA del 99.999%
- El proveedor deberá contar con una capacidad de red global de al menos 6.5 Tbps de contención

2.4 GESTION 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

ANEXOS
DIVISIÓN DE CONTRATOS

- Soporte de al menos: 3Gbps de inspección.
- Latencia máxima de 0.5 milisegundos.
- Podrá operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP.
- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, 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 hosts de la red y crear una alarma cuando cierto umbral sea rebasado.

- Funcionalidad Filtrado de Contenido Web
  - 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.
  - 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 diversas cipher suites en Secure Sockets Layer (SSL) y Transport Layer Security (TLS).
  - Deberá soportar la integración de certificados.

2.5 FIREWALL ESPECIALIZADO EN SERVICIOS WEB (WAF)

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

- Se requiere una solución que sea capaz de operar en ambientes físicos y/o virtuales en las instalaciones de la institución (On-Premise), servicios de nube como Amazon Web Services, Microsoft Azure y compatible con Google Cloud además de ofrecer la opción de protección de aplicaciones sin necesidad de instalación de hardware y/o software, es decir, como servicio.
- La solución deberá ofrecer el licenciamiento necesario para operar en cualquiera de los ambientes descritos sin necesidad de que la institución requiera adquirir hardware/software adicional y de manera ilimitada.
- En caso de que la institución requiera desplegar Appliances virtuales adicionales en nube privada y/o pública, se podrá realizar sin ningún costo adicional y de manera ilimitada.
- La solución deberá soportar cualquier aplicación web, sin importar la plataforma, tamaño del sitio, lenguaje o escenario de implementación.
- La solución deberá soportar las 80 aplicaciones Web de la institución, así como un consumo promedio mensual de 300 Mbps.
- La solución deberá ofrecer los siguientes servicios en una única plataforma integrada
- El modelo positivo de seguridad deberá definir lo que está permitido y bloquear todo lo demás. Deberá incluir direcciones URL, directorios, cookies, campos, parámetros (identificando además el formato y tipo de estos), métodos HTTP.
- Para facilitar la configuración del modelo positivo de seguridad, el dispositivo deberá aprender automáticamente la estructura y los elementos de la aplicación de manera constante y sin intervención humana.
- La configuración aprendida deberá ser accesible y modificable para el administrador de la solución.
- La solución deberá correlacionar múltiples eventos de seguridad para distinguir tráfico deseado del tráfico inadecuado.
- 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 Web. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:
    - Estado de autenticación de la sesión web
    - Por el URL de autenticación y el resultado del intento de autenticación
    - Por URL, a través del prefijo, ruta o host.
    - Por la existencia o contenido de cualquier header HTTP
    - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier personalización por expresiones regulares), ya sea en las operaciones http-request o http-response por parte del servidor Web
    - Host o dominio accedido
    - Por el protocolo usado, HTTP o HTTPS
    - Dirección IP origen
    - Por la existencia o contenido de cookies o el identificador de sesión
    - Fecha y hora del evento
    - Por usuario firmado en el aplicativo web
    - User-Agent
    - Referer-URL
    - Tiempo de respuesta o tamaño de la respuesta HTTP
- La solución deberá entregar un análisis detallado de las amenazas, incluyendo:
    - Dirección IP
    - Locación geográfica

ANEXOS
DIVISIÓN DE CONTRATOS

  - Información relevante de la sesión
- La solución deberá cubrir todas las vulnerabilidades expresadas en el OWASP Top Ten más reciente.
- El servicio deberá ser capaz de mitigar el riesgo por vulnerabilidades no parchadas tales como:
  - Command Injection
  - Clickjacking
  - Cross-Site Scripting (XSS)
  - Cross-Site Request Forgery (CSRF/XSRF)
  - Violaciones de acceso a la base de datos
  - Inyección HTML
  - Cookies Inseguras
  - Inyección JSON
  - Malformed Content-Types
  - Path Traversal
- Deberá ser reconocido como al menos "Leaders" en el The Forrester Wave: Web Application Firewalls, Q4 2017
- Deberá aparecer y ser consiste en la aparición en el cuadrante mágico de Gartner de al menos los últimos 6 años
- Red de entrega de contenido (CDN por sus siglas en inglés) con conmutación en caso de falla y redundancia
  - Almacenamiento en caché para mejoramiento de la experiencia de uso
  - Optimización de contenido entregado por la aplicación Web
  - Reglas de personalización de caché
- Balanceo global y conmutación en caso de fallas (failover) de cargas global
- Funcionales de la plataforma on-premise o virtual
- La solución deberá brindar la protección a los aplicativos cuya comunicación o publicación se limite a la red interna del instituto
- La solución deberá ser capaz de desplegarse en ambientes físico o virtual dentro de la infraestructura de la organización (On-Premise):
  - Los diferentes componentes de seguridad de los aplicativos distribuidos en red deberán de administrarse a través de una consola centralizada.
  - La solución propuesta deberá estar soportada en arquitectura de Alta Disponibilidad (HA)
  - La solución propuesta deberá tener un rendimiento de 10 Gbps.
  - La solución deberá soportar ser desplegada o implementada en línea como un puente o bridge transparente (capa 2 del Modelo OSI) las interfaces no requerirán de una dirección IP, como un proxy transparente o un proxy inverso (según se requiera), o como un analizador no en línea a través de puertos Mirror o SPAN.
  - Los Appliances físicos deberán soportar el modo bypass/fail-open/fail-closed configurable tanto para fallas de hardware como software.
  - En el modo monitoreo el administrador podrá visualizar alertas, ataques, errores de servidor y otra actividad no autorizada.
  - En el modo de cumplimiento de políticas, la solución deberá bloquear ataques proactivamente.
  - Respecto de algún ataque o alguna otra actividad no autorizada, la solución deberá ser capaz de tomar las acciones adecuadas. Las acciones deberán incluir la habilidad para terminar las solicitudes y respuestas, bloquear la sesión TCP, bloquear el usuario de la aplicación, o bloquear la dirección IP.
  - Respecto de ataques particularmente destructivos, la solución deberá ser capaz de bloquear la dirección IP por un periodo de tiempo configurable.
  - En modo analizador de paquetes, la solución deberá ser capaz de enviar un paquete TCP-RST a ambos extremos de la conexión. Alternativamente, si así se configura, la solución podrá reportar el comportamiento anómalo, pero no tomar acción alguna.

KIO Networks

DS JCHV DS JAR

- La solución podrá ser desplegada dentro de ambientes virtuales VMWare y/o Microsoft Hyper-V como dispositivo virtual.
- Los Appliances físicos deberán soportar el volumen de tráfico y deberá tener una latencia menor a 5 ms, para no impactar el desempeño de las aplicaciones.
- Para el dispositivo físico la solución deberá soportar las siguientes opciones de conectividad física por dispositivo:
  - 4 interfaces de 10 GB en Fibra Óptica tipo SX
  - Para los dispositivos físicos las interfaces de conectividad a la red deberán de ser modulares para tener la posibilidad de hacer cambios de medio como por ejemplo Cobre UTP a Fibra Óptica y viceversa, sin necesidad de cambiar el dispositivo.
  - La solución deberá proporcionar una vista unificada con el objetivo de facilitar el monitoreo todos los eventos de seguridad relacionadas con el uso de aplicaciones Web.

2.6 CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Perfil	Certificaciones a demostrar	Función	Número de recursos
Administrador del Centro de Operaciones de Seguridad (SOC 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 las aplicaciones y la infraestructura, así como prever, detectar, analizar, contener, erradicar,	Al menos 1

ANEXOS
DIVISIÓN DE CONTRATOS

Perfil	Certificaciones a demostrar	Función	Número de recursos
		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

3 FIRMAS DE ELABORACION, REVISION Y APROBACION

Atentamente

DocuSigned by:
413DA358D32D4B3...

JUAN CARLOS MARTÍNEZ VALDÉS
REPRESENTANTE LEGAL
SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.

KIO Networks

DS JCHV DS JAR

DocuSign Envelope ID: 658B6DB9-3AF3-424C-8656-941FE346D1BF

Apéndice 6

Métricas de Niveles de Servicio

SGMP_Apéndice_6

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

Ciudad de México a 13 de abril de 2022

Esta información es propiedad de Sixsigma Networks México, S.A. de C.V. (KIO NETWORKS), se proporciona con el carácter de confidencial. Esta información no será reproducida, usada o divulgada total o parcialmente por cualquier razón diferente que la de evaluar la propuesta de Servicios de KIO NETWORKS.

ANEXOS
DIVISIÓN DE CONTRATOS

ÍNDICE

1 OBJETIVO DEL DOCUMENTO 3
2 METRICA DE DISPONIBILIDAD 4
3 PENALIZACIONES Y DEDUCCIONES AL PAGO 5
3.1 Penas Convencionales 5
3.2 Deducciones por Incumplimiento de Niveles de Servicio (SLAs) 6
3.2.1 Deductivas sobre SLAs aplicables a todos los servicios del Anexo Técnico 7
4 FIRMAS DE ELABORACION, REVISION Y APROBACION 7

KIO Networks

DS JCHV DS JAR

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.

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.
  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.

ANEXOS
DIVISIÓN DE CONTRATOS

2 METRICA 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 = 100 * (TROi / (TTMi – TPFOi))

En donde:

- Disponibilidad: Se refiere a la disponibilidad de la instancia del bloque de construcción BCi que puede ser instanciado de un BCF o BCC.
- Se calculará para cada i = 1...n, de cada BCi activo en el mes, donde n es el número total de instancias activas de dichos BCs.
- Tiempo Real de Operación (TROi): Es el tiempo total durante el cual el servicio estuvo disponible durante el periodo evaluado del BCi.
- Tiempo Total Mensual (TTMi): Es el tiempo total de operación que tiene el mes respectivo del BCi.
- Tiempo Planeado Fuera de Operación (TPFOi): Es el tiempo en que el servicio se encuentra fuera de operación debido a mantenimientos planeados y programados de manera anticipada para el BCCi o BCFi. 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 las 24 horas los 7 días de la semana
- 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:

Ubicacines	Componentes de Infraestructura mensual	
Centro de Datos Primario (Ambientes Productivos y no Productivos)	Disponibilidad Directa e Indirecta *	99.982%
Extensión de Nube Privada (ATOM)	Disponibilidad Directa e Indirecta ** *	99.982%
Servicios desplegados en Instalaciones designadas por el Instituto	Disponibilidad Directa e Indirecta *	99.982%
Deficiencias en la entrega de documentación	Deficiencias en la calidad, consistencia o congruencia de la información en la	-

KIO Networks

DS JCHV DS JAR

Ubicacines	Componentes de Infraestructura mensual	
	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

** El Instituto procederá a aplicar la métrica de penalización correspondiente si el licitante incumple con la fecha compromiso registrada en la herramienta conforme al numeral 4.2.1.1.6. Mesa de servicio del Anexo Técnico.

3 PENALIZACIONES Y DEDUCCIONES AL PAGO

3.1 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.

El criterio para considerar concluida la migración desde el Centro de Datos actual hacia el Centro de Datos ofertado, será en el momento en que se encuentren los servicios descritos anteriormente activos y operando en la infraestructura propuesta por el Licitante, e interactuando con el ecosistema tecnológico institucional, esto es; con los ambientes operativos digitales productivos y no productivos instalados en los diferentes centros de datos IMSS y del Gobierno Federal así como organismos con los que interactúa el Instituto tales como SAT, RENAPO, INFONAVIT, BANCO DE MÉXICO, PROCESAR, CONSAR, BANCOS Y AFORES, entre otros, validados de conformidad por el personal que el Instituto designe (áreas de telecomunicaciones y seguridad informática, infraestructura tecnológica, desarrollo, monitoreo así como el personal de las direcciones normativas que hacen uso de los servicios en los casos que aplique).
Para el caso del incumplimiento del programa de trabajo ofertado para la implementación de los servicios por el Licitante en su propuesta, la penalización será del 2.5% (dos punto cinco por ciento) por cada día natural de atraso del costo mensual unitario de los servicios no entregados.

Durante la vida del contrato, la pena convencional por atraso en la entrega de la infraestructura adicional necesaria para dar continuidad a los servicios Institucionales será del 2.5% (dos punto cinco por ciento) por cada día natural de atraso del servicio en la entrega del costo mensual del servicio ofertado.

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, instalaciones designadas por el Instituto, pruebas en ambientes no productivos, entre otros), respecto al costo mensual del servicio

ANEXOS
DIVISIÓN DE CONTRATOS

ofertado al cual corresponda el incumplimiento, sobre las fechas establecidas de entrega, siempre y cuando sean imputables al licitante adjudicado.

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 de 0.5% (cero punto cinco) del Servicio de Soporte de Servicio de Continuidad a la Operación y Soporte de la Nube IMSS, ID 183 del formato de propuesta económica, por cada día natural de atraso

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

3.2 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.

3.2.1 Deductivas sobre SLAs aplicables a todos los servicios del Anexo Técnico

Modalidad	BCF o BCC mensual	
Centro de Datos Primario (Ambientes Productivos y no Productivos)	Disponibilidad Directa e Indirecta *	99.982%
	Deducción**por cada punto porcentual (1%)o fracción fuera del nivel de servicio	10%
Extensión de Nube Privada (ATOM)	Disponibilidad Directa e Indirecta *	99.982%
	Deducción**por cada punto porcentual (1%) o fracción fuera del nivel de servicio	10%
Servicios desplegados en Instalaciones designadas por el Instituto	Disponibilidad Directa e Indirecta *	99.982%
	Deducción**por cada punto porcentual (1%) o fracción fuera del nivel de servicio	5%
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 punto porcentual o fracción de disponibilidad fuera del nivel de servicio solicitado

4 FIRMAS DE ELABORACION, REVISION Y APROBACION

Atentamente

DocuSigned by:
413DA358D32D4B3...

JUAN CARLOS MARTÍNEZ VALDÉS
REPRESENTANTE LEGAL
SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.

KIO Networks

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

DocuSign Envelope ID: 658B6DB9-3AF3-424C-8656-941FE346D1BF

Apéndice 7

Glosario Nube IMSS

SGMP_Apéndice_7

Coordinación de Servicios de Infraestructura Tecnológica Institucional

KIO Networks

Servicio de Continuidad de Nube IMSS 2022

Ciudad de México a 13 de abril de 2022

Esta información es propiedad de Sixsigma Networks México, S.A. de C.V. (KIO NETWORKS), se proporciona con el carácter de confidencial. Esta información no será reproducida, usada o divulgada total o parcialmente por cualquier razón diferente que la de evaluar la propuesta de Servicios de KIO NETWORKS.

ANEXOS
DIVISIÓN DE CONTRATOS

ÍNDICE

1 OBJETIVO DEL DOCUMENTO 3
2 GLOSARIO 3
3 TABLA DE ACRONIMOS 7
4 FIRMAS DE ELABORACION, REVISION Y APROBACION 8

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.

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. Modelo de entrega de servicios tecnológicos cuya implementación asegura un grado mayor de continuidad operacional durante un periodo de medición determinado.

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.

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.

ANEXOS
DIVISIÓN DE CONTRATOS

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 medios electrónicos; "enrutar" los mensajes en función de quien los emite explicitando el motivo; gestionar alarmas y acciones que permitan brindar servicios 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.

CI/CD. Prácticas combinadas de integración continua y entrega continua (también conocida como despliegue continuo) que promueven la automatización de parte del proceso de desarrollo de software.

Componente Tecnológico: Se refiere a cualquier componente de un servicio, elemento de infraestructura u otro elemento que requiere ser administrado para asegurar la entrega correcta de los servicios.

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.

Contenedores. Es una tecnología que propone el empaquetamiento de una aplicación en conjunto con sus componentes y dependencias asociadas a sus tiempos de ejecución.

Despliegue. Instalación o implantación de un Activo o Servicio de TI dentro de un determinado entorno operativo.

DevOps. Es una práctica de ingeniería de software que tiene como objetivo unificar el desarrollo de software (Dev) y la operación del software (Ops). Su principal característica es promover la automatización y el monitoreo en todos los pasos de la construcción del software, desde la integración, las pruebas, la liberación hasta la implementación y la administración de la infraestructura.

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.

Elemento de Configuración (CI). Se refiere a cualquier componente de un servicio, elemento de infraestructura u otro elemento que requiere ser administrado para asegurar la entrega correcta de los servicios.

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.

DS DS
JCHV JAR

Evaluación de madurez. Es un modelo descriptivo que mide los atributos esenciales que caracterizan una organización en un nivel particular de la adopción en la gestión de cierta área de conocimiento (como puede ser la Arquitectura Empresarial o los nuevos esquemas de desarrollo como DevOps). También es un modelo normativo en el que las prácticas principales caracterizan los tipos ideales de ambiente que deberían esperarse en una organización que esté implementando gestión de dichas áreas de conocimiento.

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.

Kubernetes. Es una plataforma de contenedores portable y extensible de código abierto que se utiliza para administrar cargas de trabajo y servicios. Esta plataforma facilita la automatización y la configuración declarativa.

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.

Modelo de Gobierno. Es la disciplina que propone llevar a cabo la gestión de los diferentes componentes y servicios de TI, basada en la definición de procesos y roles alineados al cumplimiento de los objetivos de una organización.

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.

ANEXOS
DIVISIÓN DE CONTRATOS

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 ACRONIMOS

Acrónimo	Descripción
ACL	Lista de Control de Acceso (del inglés, Access Control List)
API	Interfaz de programación de aplicaciones (del inglés, *Application Programming Interface*)
BB	Bloque de Construcción (del inglés, Building Block)
BCC	Bloques de Construcción Comunes
BCF	Bloques de Construcción Fundamentales o componente de infraestructura
CAB	Consejo Consultor de Cambios (del inglés, Change Advisory Board)
CAT	Centro de Arquitectura Tecnológica
CDP	Centro de Datos Primario
CI	Elemento de configuración (del Inglés *Configuration Item*)
CI/CD	Integración Continua / Desarrollo Continuo
CCTV	Circuito Cerrado de Televisión
CMDB	Base de Datos de Elementos de Configuración (del inglés, Configuration Management Database)
DIDT	Dirección de Innovación y Desarrollo Tecnológico
DRP	Plan de Recuperación en caso de Desastres (del Inglés, Disaster Recovery Plan)
ECAB	Consejo Consultor de Cambios Emergentes (del inglés, Emergency Change Advisory Board)
EDN	Estrategia Digital Nacional
EN	Escritorios en la Nube
ENH	Extensión de Nube Híbrida
ENP	Extensión de Nube Privada
GB	Gigabytes (métrica para cuantificar una capacidad de almacenamiento de información digital)
Gbps	Gigabits por Segundo (métrica para cuantificar la velocidad de transmisión de información entre dos sistemas digitales)
HSM	Módulo de Seguridad en Hardware (del Inglés *Hardware Security Module*)
IaaS	Infraestructura como un Servicio (del inglés, Infrastructure as a Service)
IMSS	Instituto Mexicano del Seguro Social
ISO	Organización Internacional para la Estandarización (del inglés, International Organization for Standardization)
ISP	Proveedor de Servicios de Internet (del inglés, Internet Service Provider)
ITIL	Biblioteca de Infraestructura de Tecnologías de Información (del inglés, Information Technology Infrastructure Library)
LAN	Red de Área Local (del inglés, Local Area Network)
LED	Diodo Emisor de Luz (del inglés, Light Emisor Diode)
MAAGTICSI	Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información
MB	Megabytes
Mbps	Megabits por Segundo
MOSNI	Marco Operativo de los Servicios de Nube IMSS
MPLS	Conmutación Multi-Protocolo mediante Etiquetas (del inglés, Multiprotocol Label Switching)
MTR	Marco Tecnológico de Referencia
NIST	National Institute of Standards and Technology

ANEXOS
DIVISIÓN DE CONTRATOS

Acrónimo	Descripción
OLA	Acuerdos de Nivel de Operación (del inglés, Operational Level Agreement)
PaaS	Plataforma como un Servicio (del inglés, Platform as a Service)
PAN	Puntos de Acceso a la Nube
PDA	Asistente Digital Personal (del inglés, Personal Digital Assistant)
PEP	Portafolio Estratégico de Proyectos
PND	Plan Nacional de Desarrollo
RFC	Solicitud de Cambio (del inglés, Request for Change)
RFI	Solicitud de información (del inglés, Request for information)
RPO	Punto Objetivo de Recuperación, por sus siglas en inglés
RTO	Tiempo Objetivo de Recuperación, por sus siglas en inglés
SaaS	Software como un Servicio (del inglés, Software as a Service)
SCO	Servicio de Continuidad Operativa
SDI	Servicios desplegados en Instalaciones designadas por el Instituto
SLA	Acuerdos de niveles de servicios (del inglés, Service Level Agreement)
TB	Terabytes
TIC	Tecnologías de Información y Comunicaciones
UANP	Usuario de Acceso a la Nube Privada
UGD	Unidad de Gobierno Digital
VRF	Virtual Routing and Forwarding por sus siglas en inglés

4 FIRMAS DE ELABORACION, REVISION Y APROBACION

Atentamente

DocuSigned by:
413DA358D32D4B3...

JUAN CARLOS MARTÍNEZ VALDÉS
REPRESENTANTE LEGAL
SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.

KIO Networks

DS JCHV DS JAR

DocuSign Envelope ID: 47B57195-AD1A-465D-B7B6-0950D030E160

Apéndice

Detalle de Servicios

SGMP_Apéndice

Coordinación de Servicios de Infraestructura Tecnológica Institucional

Servicio de Continuidad de Nube IMSS 2022

Ciudad de México a 13 de abril de 2022

Esta información es propiedad de Sixsigma Networks México, S.A. de C.V. (KIO NETWORKS), se proporciona con el carácter de confidencial. Esta información no será reproducida, usada o divulgada total o parcialmente por cualquier razón diferente que la de evaluar la propuesta de Servicios de KIO NETWORKS.

ANEXOS
DIVISIÓN DE CONTRATOS

ÍNDICE

1 OBJETIVO DEL DOCUMENTO 3
2 SERVICIOS 3
2.1 Servicio de Continuidad a la Operación y Soporte 4
2.1.1 Soporte a la Continuidad Operativa 4
2.1.2 Consumo de BCFs para el Servicio 37
2.1.3 Plataformas para el Servicio de Continuidad a la Operación y Soporte 37
2.1.4 Servicios eventuales para la Continuidad a la Operación y Soporte 39
2.1.5 Servicios extendidos 39
2.1.6 Servicio de soporte de Extensión de Nube Privada 39
2.2 Servicios de Continuidad y Soporte de Telecomunicaciones 39
2.2.1 Plataformas de Servicios de Telecomunicaciones 39
2.2.1.1 Punto Neutro 39
2.2.2 Servicios eventuales 50
2.2.3 Servicios extendidos 50
2.3 Servicio de Continuidad y Soporte de Seguridad 51
2.3.1 Soporte para la Operación de la Seguridad de la Nube IMSS 51
2.3.2 Servicios eventuales de seguridad 61
2.3.3 Servicios extendidos 61
2.4 Servicio de Gestión de Medición del Desempeño de Aplicativos y Componentes Institucionales 61
2.4.1 De la fase de diagnóstico inicial del estado de aplicativos y componentes Institucionales: 62
2.4.2 De la fase de optimización del estado actual para mejora del desempeño óptimo: 62
2.4.3 De la fase de propuesta para su implementación en un estado mínimo funcional: 63
2.5 Migración del Centro de Datos Actual al Centro de Datos Ofertado por el KIO Networks (en caso de aplicar) 64
2.6 Elementos comunes de los servicios 66
2.6.1 Servicio de Infraestructura y Bloques de Construcción Fundamentales. 66
2.6.2 UNIDADES DE SOPORTE EXTENDIDO 68
2.6.3 Servicio de Soporte Extendido para el Centro de Cómputo 68
2.6.4 Descripción del Servicio 68
2.6.5 Mecanismo de consumo de las Unidades de Soporte Extendido 68
2.6.6 Modalidad de Proyecto y Servicio de Soporte Extendido 69
3 FIRMAS DE ELABORACION, REVISION Y APROBACION 69

1 OBJETIVO DEL DOCUMENTO

Describir el contenido de los servicios solicitados por el Instituto y que el Licitante adjudicado deberá brindar durante la vigencia del servicio.

Para efectos del anexo técnico y sus apéndices se entenderá como Bloque de Construcción Fundamental (BCF) a cualquier componente mínimo tecnológico de Infraestructura.

2 SERVICIOS

KIO Networks comprende que el Instituto solicita los servicios que le permitan garantizar la continuidad operativa de los diferentes dominios tecnológicos que soportan los procesos de negocio de sus Direcciones Normativas. KIO Networks con base en el detalle de los diferentes apéndices que integran el presente Anexo técnico elaborará la propuesta técnica para dar cobertura a las necesidades que se plantean, dicha propuesta se elaborará en el marco de las mejores prácticas de la industria en materia de Tecnologías de Información, Comunicaciones y Seguridad de la Información. Los servicios requeridos que se mencionan a continuación se detallan más adelante en el presente Apéndice:

- Servicio de Continuidad Operación y Soporte
- Servicio de Continuidad y Soporte a la Seguridad
- Servicios de Integralidad y Comunicaciones

KIO Networks independientemente de ofertar los tres servicios que anteceden en caso de resultar adjudicado, incluirá en la propuesta un servicio diseñado con personal calificado para que colabore de manera cotidiana con el administrador del contrato y el grupo de gobierno en lo que corresponde a la identificación oportuna de asuntos relacionados con la alineación estratégica de los tres servicios mencionados. Asimismo, dicho personal se encargará de preparar un reporte ejecutivo del avance de cada servicio y su contribución estratégica, también realizará recomendaciones de gestión y atención a los asuntos que le sean requeridos por el administrador del contrato.

Entre otras tareas, el personal asignado por KIO Networks se encargará de gestionar todos los requerimientos del administrador del contrato y el grupo de gobierno asegurándose de dar seguimiento de su atención hasta su conclusión, la información resultante será parte invariablemente del reporte ejecutivo mensual o con la periodicidad que le requiera el referido administrador.

Este personal especializado y el administrador del contrato deberán formular las estrategias que permitan explotar las tecnologías digitales para maximizar la eficacia y la eficiencia de la solución y la capacidad de respuesta para alinear la arquitectura que resulte de su propuesta técnica a lo establecido por la Coordinación Nacional de Estrategia Digital, en materia de contenerización de los servicios entre otras.

Adicionalmente, el personal asignado por el Licitante en coordinación con el administrador del contrato se deberá involucrar en la planeación y ejecución de los proyectos inscritos en el Portafolio de Proyectos de Tecnologías de Información (POTIC) para proponer soluciones tecnológicas que habiliten las iniciativas de las Direcciones Normativas que requieran servicios en el alcance del presente anexo técnico, siempre bajo la directriz del Administrador del contrato.

KIO Networks presenta y se obliga en la propuesta técnica a la totalidad de lo solicitado en el Apéndice, tomando como base todas y cada una de las especificaciones técnicas, condiciones y requerimientos que se indican en el mismo.

ANEXOS
DIVISIÓN DE CONTRATOS

2.1 Servicio de Continuidad a la Operación y Soporte

2.1.1 Soporte a la Continuidad Operativa

KIO Networks en caso de resultar adjudicado brindará continuidad operativa, gestión, operación, puesta a punto (tunning), configuración y soporte a a la Infraestructura, 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 especializado y soluciones tecnológicas suficientes para la entrega del servicio.

KIO Networks en caso de resultar adjudicado, 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.

KIO Networks habilitará el servicio de monitoreo de la infraestructura con la que brinda sus servicios de centros de datos, no solo en el ámbito de infraestructura encendida, sino que también debe brindar el monitoreo del desempeño de los aplicativos, estos son, experiencia de usuario de los principales aplicativos institucionales, conforme el personal del gobierno del contrato le defina a **KIO Networks**. Adicionalmente, **KIO Networks** permitirá al IMSS al acceso a sus servicios de monitoreo a fin de concentrar la información de monitoreo de los diferentes servicios en un sistema central de monitoreo IMSS.

KIO Networks efectuará todas las acciones necesarias para interconectar su mesa de servicios con la mesa de servicios institucional IMSS, a efecto de que el intercambio de información de al menos 2200 tickets mensuales en promedio (esta cantidad puede variar dependiendo de los niveles de servicio y continuidad que presente la infraestructura entregada)entre ambos sistemas de mesa de servicios sean de manera automatizada en un plazo máximo de 30 días posteriores al fallo, para lo cual deberá entregar un plan de trabajo y efectuar reuniones al menos semanales para coordinar estas labores de integración de mesas de servicio.

2.1.1.1 GESTION 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.

KIO Networks alineará la prestación de los servicios a través de los procesos basados en las mejores prácticas de ITIL v3 o superior, identificando las actividades que se pueden mejorar u optimizar, por lo que **KIO Networks** contará con personal que tenga los conocimientos y experiencia necesaria en el manejo de los siguientes procesos para él su desarrollo e implementación:

- Gestión de eventos
- Gestión de requerimientos
- Gestión de incidentes
- Gestión de problemas
- Gestión de cambios
- Gestión de configuraciones

- Gestión de liberaciones

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

2.1.1.1.1 GESTION DE EVENTOS

Se entenderá como "evento" todo cambio de estado significativo de un elemento de configuración, BCF, 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, 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 el alcance de umbrales operativos.

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

La gestión de la operación de los servicios ofertados por el licitante incluyendo la administración de los eventos deberá operar las 24 horas del día de los 7 días de la semana durante a vigencia del servicio 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 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.

KIO Networks, en el monitoreo proactivo, considerará la identificación de infraestructura, métricas adecuadas para cada infraestructura implementada, la definición de los umbrales óptimos y la correlación entre las alertas, 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 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), software, middleware, bases de datos y 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 y detallados hacia **KIO Networks|**, los cuales estarán relacionados de manera ordenada en la **CMDB** y que, de manera conjunta entre el Instituto y **KIO Networks** establecerán en una mesa de trabajo la profundidad, alcance, insumos y revisión de la integración entre los componentes a ser monitoreados.

Actividades enunciativas más no limitativas soportadas por el proceso:

ANEXOS
DIVISIÓN DE CONTRATOS

- Detección de los eventos.
- Filtrado de los eventos.
- Registro de los eventos (fecha y hora de apertura)
- Correlación de los eventos.
- Priorización de los eventos.
- Atención/solución de los eventos (fecha y hora de solución)
- Documentación de los eventos
- Cierre de los eventos

KIO Networks contemplará la implementación de una herramienta en donde se deberán registrar los tickets de tipo "Evento", con el fin de mantener un control en la volumetría y ser la base para el desarrollo y construcción de KPIs. Para resolver los eventos, **KIO Networks** considerará las prioridades que se establezcan con base al impacto y a la urgencia asignada al evento.

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

KIO Networks asignará un Gestor del Proceso de Gestión de Eventos que vigile el apego al proceso establecido y lleve a cabo las actualizaciones necesarias con base a las necesidades de la operación.

KIO Networks 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.
- Número de incidente en caso de derivación al proceso de gestión de incidentes

KIO Networks en caso de resultar adjudicado, mantener actualizada la CMDB y con accesos permanentes a personal del IMSS, a efecto de servir como:

- Biblioteca actualizada de elemento (BCF) para la toma de decisiones en caso de incidencias, actualizaciones tecnológicas, medición de impactos, experiencia de usuario,
- Diagramas de arquitectura tecnológica de referencia en la operación, mejora continua, incidentes, actualizaciones tecnológicas,
- Documento de diseño de aplicaciones o en su caso, de interconexión entre aplicativos, bases de datos o hacia entidades internas y externas.
- Inventario de infraestructura y sus correspondientes infraestructuras físicas y virtuales (licenciamiento y configuración de recursos lógicos)
- Correlación con la Base de datos de conocimiento de la operación de los servicios tecnológicos institucionales.

2.1.1.1.2 GESTION DE REQUERIMIENTOS

Se entenderá como "requerimiento" aquella petición documental por parte del Instituto hacia **KIO Networks** respecto al alcance de los servicios, servicios de continuidad, servicios de integralidad y servicios de seguridad descritos en el presente anexo técnico. No se considerarán requerimientos los incidentes, problemas, eventos, modificaciones a la CMDB, solicitudes de cambio normales, estándar y emergentes ni requerimientos de infraestructura a ser implementada.

KIO Networks proporcionará un punto único de entrada para todos los requerimientos que no implican un incidente, tales como accesos, permisos, requerimientos de información o cualquier requerimiento relacionado a los servicios del presente anexo técnico.

KIO Networks en caso de resultar adjudicado, proporcionará un medio de comunicación para recibir los requerimientos de manera formal por parte del Instituto el cual será el correo electrónico.

Actividades enunciativas más no limitativas soportadas por el proceso a cargo de **KIO Networks:**

- Operar la solución tecnológica para la gestión de requerimientos
- Gestionar la solicitud.
- Asegurar la atención de la solicitud
- Registro de los requerimientos (fecha y hora de apertura)
- Priorización de los requerimientos.
- Asignación de los requerimientos.
- Atención/solución de los requerimientos (fecha y hora de solución)
- Documentación de los requerimientos.
- Cierre de los requerimientos.

KIO Networks contemplará la implementación de una herramienta en donde se deberán registrar los tickets de tipo "Requerimiento", con el fin de mantener un control en la volumetría y ser la base para el desarrollo y construcción de KPIs. Para atender los requerimientos, **KIO Networks** considerará las prioridades en conjunto con el Instituto.

KIO Networks asignará un Gestor del Proceso de Gestión de Requerimientos que vigile el apego al proceso establecido y lleve a cabo las actualizaciones necesarias con base a las necesidades de la operación.

KIO Networks en caso de resultar adjudicado, 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 para la atención del requerimiento.

ANEXOS
DIVISIÓN DE CONTRATOS

2.1.1.1.3 GESTION 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, o plataforma, aunque no haya impactado en el servicio.

El proceso deberá restablecer la operación normal del servicio tan rápido como sea posible, minimizando el impacto adverso en los componentes, aplicaciones, servicios u otros componentes.

Para resolver los incidentes, **KIO Networks** considerará las prioridades que se establezcan con base al impacto y a la urgencia asignada al incidente.

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 a este proceso, sugerencias de mejora.

Será considerado un **Incidente Mayor** aquel que deja fuera de operación al menos un servicio crítico del Instituto o algún BCF que afecte de manera colateral otros servicios o aplicaciones, BCF considerados transversales, fallas masivas de red, o cualquier servicio que el Instituto haga de conocimiento a **KIO Networks** y que tenga una afectación "total" a nivel nacional.

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/o mesas de trabajo especializadas para la atención de incidentes (WarRooms).

KIO Networks definirá grupos de soporte especializados de primer, segundo o tercer nivel de atención según corresponda para la solución de los incidentes y el restablecimiento del servicio tan pronto sea posible.

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 en caso de resultar adjudicado, habilitará mecanismos de comunicación agiles (foros sociales, herramientas móviles de comunicación, etc.) para el seguimiento del incidente (incluyendo los mayores) e informar en un resumen final por mecanismos de comunicación formales que el Instituto acuerde con **KIO Networks** (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 **KIO Networks**.

Para la gestión de incidentes, **KIO Networks** efectuará de manera enunciativa más no limitativa, las siguientes actividades durante el incidente:

- Notificar en tiempo y forma al Instituto la materialización del incidente por el mecanismo de comunicación ágil.
- Coordinar la solución del incidente y de ser necesario en conjunto con el Instituto.
- Notificar en tiempo y forma los avances respecto a la solución del incidente.
- Notificar la solución aplicada para la solución del incidente.

KIO Networks entregará, en un plazo no mayor a 72 horas posterior a la solución del incidente, un reporte de análisis llamado **"post-mortem" o "Reporte de incidente"** del **"incidente mayor"** presentado o de aquel 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 afectados de manera directa e indirecta, misma que será analizada, revisada y en su caso modificada por parte del Instituto.

El reporte post-mortem deberá contener al menos de manera enunciativa mas no limitativa lo siguientes rubros:

Cronología del Incidente desde su detección, notificación, acciones, grupos participantes, hasta su solución
Lista de BCFs, afectados de manera directa e indirecta
Número y título del incidente.
Fecha del incidente.
Tiempo de solución del incidente.
Cronología de las acciones de restauración llevadas a cabo para la solución del incidente.
Componentes, aplicaciones, o servicios que se vieron afectados a causa del incidente desglosados en BCFs
Duración del incidente (detallado por BCF afectado).
Acciones de mejora o recomendaciones (si aplican).
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.
- Registro de los incidentes (fecha y hora de apertura).
- Identificar y registrar los incidentes.
- Categorizar, priorizar y realizar diagnóstico inicial.
- Investigar y diagnosticar.
- Solucionar de los incidentes (fecha y hora de solución) y recuperar.
- Documentación de los incidentes.
- Cerrar el incidente.
- Informar al Instituto el estado de los incidentes.

KIO Networks asignará un Gestor del Proceso de Gestión de Incidentes que vigile el apego al proceso establecido y lleve a cabo las actualizaciones necesarias con base a las necesidades de la operación.

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 reporte 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 (brigdes telefónicos, foros de comunicación ágil, foros móviles etc.).
- Abrir los canales de comunicación necesarios para la atención de incidentes (brigdes telefónicos, foros de comunicación ágil, foros móviles etc.)

Aquellos incidentes que no se conozca la causa raíz que lo originó, se deberá proceder asociar un folio de tipo "problema" para iniciar con la investigación y búsqueda de causa raíz, haciendo uso del proceso de Gestión de Problemas.

ANEXOS
DIVISIÓN DE CONTRATOS

KIO Networks contemplará la implementación y operación de una herramienta, en donde se deberán registrar los tickets de tipo "Incidente y/o restauraciones de servicio", con el fin de mantener un control en la volumetría y ser la base para el desarrollo y construcción de KPIs.

Para resolver los incidentes, **KIO Networks** considerará las prioridades que se establezcan con base al impacto y a la urgencia asignada al incidente.

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

KIO Networks en caso de resultar adjudicado, 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 afectados de manera directa e indirecta.

KIO Networks asignará un Gestor del Proceso de Gestión de Incidentes que vigile el apego al proceso establecido y lleve a cabo las actualizaciones necesarias con base a las necesidades de la operación.

2.1.1.1.4 GESTION 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 o los incidentes.

KIO Networks analizará y encontrar la causa raíz que ocasionan los eventos e incidentes recurrentes, realizar actividades proactivas para detectar y prevenir futuros incidentes y atender el registro de errores conocidos que permita el diagnóstico de una manera más ágil.

KIO Networks registrará un nuevo problema por uno o varios incidentes recurrentes y 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 personal especializado para el análisis y diagnóstico de los problemas, conformados por especialistas en las tecnologías descritas en el presente anexo, con el objeto de encontrar la causa raíz origen y aplicar las remediaciones necesarias para evitar la recurrencia.

Para la gestión de los problemas, **KIO Networks** efectuará de manera enunciativa más no limitativa, las siguientes actividades:

- Administrar y resguardar la base de datos de conocimiento y/o la base de datos de errores conocidos.
- Realizar el análisis de las recurrencias de los incidentes para evitar la presencia de incidentes mayores.

KIO Networks entregará al Instituto al término de la investigación y diagnóstico del problema y previo al cierre del mismo, un reporte con todas las acciones llevadas a cabo en la solución del problema, dicho reporte será un "dictamen" el cual contendrá de manera enunciativa mas no limitativa los siguientes rubros:

- Número y título del problema.
- Fecha de apertura del problema.
- Servicios, componentes o aplicaciones intervenidos en la solución del problema.
- Número(s) de incidente(s) asociado(s) al problema (problemas reactivos).
- Cronología de las acciones llevadas a cabo para la solución del problema.
- Número(s) de cambios aplicados y asociados al problema
- Descripción de cada cambio y su beneficio u objeto.
- Acciones de mejora o recomendaciones y/o riesgos asociados (si aplica)
- Fecha de cierre del problema.

Para aquellos problemas que no puedan ser solucionados, **KIO Networks** establecerá en el reporte "dictamen" el riesgo asociado al problema.
Actividades enunciativas más no limitativas a cargo de **KIO Networks**

- Registro de los problemas (fecha y hora de apertura).
- Categorización de los problemas.
- Priorización de los problemas.
- Asignación de los problemas.
- Operar la solución tecnológica para la gestión de problemas.
- Gestionar la solución de problemas.
- Investigación y diagnóstico de los problemas
- Solución de los problemas (fecha y hora de solución
- Documentar el problema en conjunto con el Instituto.
- Generar informes del seguimiento del problema.
- Documentar el cierre del problema.

KIO Networks asignará un Gestor del Proceso de Gestión de Problemas que vigile el apego al proceso establecido y lleve a cabo las actualizaciones necesarias con base a las necesidades de la operación.

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.

ANEXOS
DIVISIÓN DE CONTRATOS

- Cantidad de incidentes recurrentes.
- Cambios asociados al problema.
- Acciones semanales para identificar la causa raíz.
- Incidentes resueltos sin causa raíz detectada.

Actividades enunciativas más no limitativas soportadas por el proceso:

- Registro de los problemas (fecha y hora de apertura).
- Categorización de los problemas.
- Priorización de los problemas.
- Asignación de los problemas.
- Investigación y diagnóstico de los problemas.
- Solución de los problemas (fecha y hora de solución)
- Documentación de los problemas.
- Cierre de los problemas.

KIO Networks contemplará la implementación de una herramienta, en donde se deberán registrar los tickets de tipo "Problema", con el fin de mantener un control en la volumetría y ser la base para el desarrollo y construcción de KPIs.

2.1.1.1.5 GESTION 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, 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. Los Requerimientos de Cambios de tipo estándar ya serán pre-aprobados, pero 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 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 se definirá en conjunto con el Instituto durante las mesas de planeación del arranque y que podrá modificarse durante la vigencia del contrato.

KIO Networks participará en los comités de cambios calendarizados por parte del Instituto (CAB).

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.

KIO Networks categorizará los cambios en Normales, Estándar y Emergentes de acuerdo con 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 que pudieran afectar la disponibilidad de los servicios.

KIO Networks asegurará que los cambios sean registrados, evaluados, autorizados, priorizados, planeados, probados, implementados, documentados y revisados de una forma controlada.

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

Para la gestión de los cambios, **KIO Networks** efectuará de manera enunciativa más no limitativa, las siguientes actividades durante la ejecución del cambio:

- Notificar el inicio de la ejecución del cambio
- Notificar el término de la ejecución del cambio.
- Notificar el resultado del cambio.

KIO Networks designará un **Gestor de Cambios** que será el coordinador y responsable de que todos los cambios se gestionen de acuerdo con el proceso que se establezca en conjunto con el Instituto y lleve a cabo las actualizaciones necesarias con base a las necesidades de la operación. El Gestor de Cambios será en enlace con el Instituto para los cambios.

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

Actividades a cargo de **KIO Networks**

- Registro de los cambios (fecha y hora de apertura)
- Asegurar que los cambios sean registrados, evaluados, autorizados, priorizados, planeados, probados, implementados, documentados y revisados de una forma controlada.
- Categorización de los cambios.
- Planear y controlar los cambios.
- Participar en la planeación.
- Priorización de los cambios.
- Asignación de los cambios.
- 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.
- Ejecución de los cambios (fecha y hora de ejecución
- 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
- Documentación de los cambios
- Cierre de los cambios.

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

ANEXOS
DIVISIÓN DE CONTRATOS

KIO Networks contemplará la implementación de una herramienta, en donde se deberán registrar los tickets de tipo "Cambio", con el fin de mantener un control en la volumetría y ser la base para el desarrollo y construcción de KPIs.

Para la ejecución de los cambios, **KIO Networks** considerará las prioridades que se establezcan, así como el riesgo identificado al cambio.

2.1.1.1.6 MESA DE SERVICIO

KIO Networks contará con una Mesa de Servicios para recibir, registrar, categorizar generar información de los procesos y dar seguimiento a los tickets generados con base a 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. Dicha Mesa de Servicios deberá estar apegada a las mejores prácticas de ITIL v3 o superior.

La Mesa de Servicio servirá como punto único de contacto para recibir cualquier evento relacionado con la operación del servicio.

La principal función de la Mesa de Servicio será brindar un soporte a los usuarios que el Instituto defina (se definirá en las mesas de trabajo la lista de usuarios autorizados) proporcionando una solución que permita la continuidad de la operación de los servicios del Instituto basado en la gestión de ITSM.

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

- Solicitud de reportes y/o información.
- Requerimientos que estén al alcance de **KIO Networks**.
- Fallas de hardware en los servidores suministrados al Instituto.
- Degradación de servicio en las aplicaciones o servicios del Instituto.
- Fallas y/o degradación de funcionamiento en Sistema Operativos, Bases de Datos, Aplicativos, etc.
- Fallas y/o degradación en los servicios de telecomunicaciones.
- Fallas en el software de monitoreo.
- Cualquier otro elemento soportado o administrado por **KIO Networks**.

KIO Networks categorizará y asignará en tiempo y forma los tickets solicitados por el Instituto, mismo que una vez registrado el ticket deberá contener de manera enunciativa mas no limitativa lo siguiente:

- Número de ticket.
- Nombre del solicitante.
- Servicio afectado
- Breve descripción (Síntoma, Evidencia)
- Resumen.
- Prioridad asignada al ticket con base al impacto y la urgencia.
- Grupo de soporte asignado el ticket.
- Categorización del ticket
- Fecha y hora de apertura.

KIO Networks considerará todo lo necesario para llevar a cabo la Integración de su Mesa de Servicio 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.

KIO Networks efectuará todas las acciones necesarias para conectar su mesa de servicios con la mesa de servicios institucional IMSS, a efecto de que el intercambio de información entre ambos sistemas de mesa de servicios sea

de manera automatizada en un plazo máximo de 30 días posteriores al fallo, para lo cual deberá entregar un plan de trabajo y efectuar reuniones al menos semanales para coordinar estas labores de integración de mesas de servicio.

La Mesa de Servicio deberá estar disponible para atender y gestionar los tickets las 24 horas del día de los 7 días de la semana durante la vigencia del servicio. **KIO Networks** será responsable de contar con los agentes necesarios para atender la demanda en los diferentes turnos.

La Mesa de Servicios deberá fungir como primer nivel de soporte en la solución de los tickets, en caso de no poder solucionar, deberá ser asignado hacia los siguientes niveles de soporte establecidos (segundo o tercer nivel según corresponda).

La Mesa de Servicios deberá contemplar las siguientes actividades de manera enunciativa mas no limitativa:

- Fungir como punto único de contacto para el seguimiento y gestión del ticket
- Fungir como punto único de contacto para el seguimiento y gestión del ticket.
- Atender los correos electrónicos recibidos así como la atención de las llamadas telefónicas.
- Registrar y clasificar los tickets en la herramienta de gestión incluyendo el horario en que sean creados.
- Proporcionar el primer nivel de soporte (nivel 1) para la atención inmediata del ticket.
- Dar seguimiento de inicio a fin en la resolución y/o atención del ticket, pasando por cualquier área de soporte (N2 y/o N3) hasta la solución y cierre del mismo.
- Asegurar cada una de las fases por las que pasa el ticket dentro de la herramienta de gestión, con el fin de garantizar el cumplimiento del Acuerdo de Nivel de Servicio.
- Integrar a los distintos grupos de soporte en las conferencias para la atención y solución del ticket.
- Aplicar los niveles de escalación con base a los procesos establecidos.

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.

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.

En el caso de la Modalidad M5 Instalaciones designadas por el Instituto, y derivado de que se trata de BCF´s que no estarán bajo la administración del licitante adjudicado, los ticket se atenderán de acuerdo a lo siguiente

- La herramienta de la mesa de servicio del licitante o del Instituto deberá tener configurado el servicio de atención de soporte para la modalidad M5
- Los usuarios del servicio registrarán en la mesa de ayuda correspondiente el ticket que contenga el reporte con la incidencia o solicitud de servicio de que se traté.
- El licitante tendrá 48 horas para llevar a cabo el diagnóstico y solución correspondiente registrándolo en la herramienta para evitar penalizaciones.

2.1.1.1.7 PROCESO DE GESTION DE LIBERACIONES

ANEXOS
DIVISIÓN DE CONTRATOS

El proceso de Gestión de Liberaciones tiene como objeto llevar a cabo la planificación, programación y control de las liberaciones que son requeridas por el Instituto al tiempo que protege la integridad de los servicios existentes.

KIO Networks en caso de resultar adjudicado, será responsable del soporte de las aplicaciones, módulos o herramientas que le hayan sido transferidas, garantizando la correcta y óptima operación de las mismas durante el proceso de transición y a lo largo de la vigencia del contrato, aplicando las buenas prácticas de TI y alineados a los procesos de gestión de: cambios, liberaciones, eventos, requerimientos, configuración, incidentes y problemas.

KIO Networks a través del proceso de Gestión de Liberaciones, será responsable de la instalación de paquetes aplicativos provenientes de proyectos, requerimientos de operación o las derivadas a las aplicaciones, módulos o herramientas que le hayan sido transferidas por el Instituto a **KIO Networks**.

KIO Networks, a través del proceso de Gestión de Liberaciones, será responsable de la toma de la administración y soporte del aplicativo, componente tecnológico o cualquier otro elemento que transfiera el Instituto a **KIO Networks**, siguiendo y respetando las políticas, lineamientos y actividades descritas en el Proceso de Gestión de Liberaciones.

KIO Networks considerará aspectos tales como:

- Definir y acordar, en conjunto con el Instituto los planes de liberación e implementación.
- Crear y probar los paquetes de liberación que considere el Instituto previo a la implementación.
- Implementar los paquetes de liberación al ambiente de producción siguiendo un plan y calendario acordados con el Instituto.
- Asegurar que todos los paquetes de liberación puedan ser instalados, probados, verificados y/o desinstalarse o removerse de ser necesario en conjunto con el Instituto.
- Asegurar que los servicios se encuentren disponibles una vez que los usuarios finales lo confirmen a través del área operativa del Instituto.

Se deberá solicitar al Instituto el Proceso de Gestión de Liberaciones con su respectivas políticas que establecen los roles y responsabilidades así como las guías y detalles para cada sistema o servicio.

Actividades enunciativas mas no limitativas soportadas por el proceso a cargo de **KIO Networks:**

- Invocación al proceso de Gestión de Cambios.
- Invocación al proceso de Gestión de Configuraciones.
- Invocación al proceso de Gestión de Eventos.
- Invocación al proceso de Gestión de Incidentes.
- Entrega de componente, servicio o aplicativo a soportar por parte de **KIO Networks**.
- Asegurar la correcta transferencia de conocimiento a **KIO Networks** del producto o servicio a soportar.

El Instituto deberá proporcionar a **KIO Networks** toda la documentación relacionada con el soporte, operación, administración y funcionalidad del servicio, incluyendo los niveles de escalación al interior del Instituto.

KIO Networks asignará un Gestor del Proceso de Gestión de Liberaciones que vigile las actividades para la entrega-recepción del servicio que será administrado por **KIO Networks**.

2.1.1.1.8 PROCESO DE GESTION DE CONFIGURACIONES

Tiene como propósito brindar un modelo lógico de los Elementos de Configuración (CI) que participan en la prestación de un servicio de TI, incluyendo las relaciones entre los mismos; mediante la identificación, control,

mantenimiento y verificación a lo largo de su vida útil. Con el fin de proporcionar información a los diferentes procesos de gestión del servicio para la toma de decisiones.

Para la gestión de configuraciones, **KIO Networks** efectuará de manera enunciativa más no limitativa, las siguientes actividades:

- Identificar todos los componentes de infraestructura que soportan los servicios de TI ubicados en el Site de **KIO Networks**
- Vigilar que los elementos de configuración (CI´s) se encuentren registrados en la CMDB y sean identificados de manera única.
- Generar diagramas de arquitectura de los servicios de TI que se encuentran ubicados en el Site de **KIO Networks** y permita visualizar las relaciones entre los elementos de configuración (CI´s).
- Vigilar que la información de los elementos de configuración (CI´s) registrados en la CMDB, sea precisa y confiable, en caso de encontrar incoherencias, realizar las actividades de corrección.
- Proporcionar inventario de la infraestructura bajo solicitud del Instituto.

La solución implementada por **KIO Networks** 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** 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. **KIO Networks** asignará un Gestor del Proceso de Gestión de Configuraciones que vigile el apego al proceso establecido y lleve a cabo las actualizaciones necesarias con base a las necesidades de la operación.

KIO Networks mantendrá actualizada la CMDB y con accesos permanentes a personal del IMSS, a efecto de servir como:

- Biblioteca actualizada de elemento (BCF) para la toma de decisiones en caso de incidencias, actualizaciones tecnológicas, medición de impactos, experiencia de usuario,
- Diagramas de arquitectura tecnológica de referencia en la operación, mejora continua, incidentes, actualizaciones tecnológicas,
- Documento de diseño de aplicaciones o en su caso, de interconexión entre aplicativos, bases de datos o hacia entidades internas y externas.
- Inventario de infraestructura y sus correspondientes infraestructuras físicas y virtuales (licenciamiento y configuración de recursos lógicos)
- Correlación con la Base de datos de conocimiento de la operación de los servicios tecnológicos institucionales.

2.1.1.2 GESTIÓN DE SOPORTE A LA OPERACIÓN

2.1.1.2.1 ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

La administración de sistemas operativos contempla la gestión, instalación, configuración, puesta a punto, 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.

ANEXOS
DIVISIÓN DE CONTRATOS

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 del presente Anexo Técnico:

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 marco de referencia que utiliza el Instituto; 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, actualización de versiones, aplicación de parches y fixes, 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, alineado al marco de referencia ITIL solicitado en este anexo Técnico.

d) **KIO Networks** comunicará y coordinará a través del Proceso de Gestión de Cambios del Instituto aquellos cambios planeados en las funcionalidades, actualización de versiones, aplicación de parches, fixes 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.

i) 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, virtual a contenedores para microservicios (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 incluyendo configuraciones, accesos, arquitecturas o lo que el Instituto determine sea requerido para las migraciones en comento, Asimismo, deberá realizar la creación y administración de plantillas (Templates) que se requieran de dichos ambientes.

j) **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 estas 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.

k) **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.

l) **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.

m) **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 Grupo de Control de Cambios 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.

2.1.1.2.2 ADMINISTRACIÓN DE BASE DE DATOS

KIO Networks será responsable de la instalación, puesta a punto, gestión, administración, actualización de versiones, aplicación de parches y fixes y soporte de las Bases de Datos, manejadores, instancias, así como el software relacionado, tales como: DB2, Oracle, SQL server, PostgreSQL, Mongo DB, Cassandra, entre otros que defina el Instituto durante la vida del contrato, en cualquiera de los ambientes soportados por el presente anexo técnico.

La instalación, puesta a punto, gestión, administración, actualización de versiones, aplicación de parches y fixes y soporte de las Bases de Datos, manejadores, instancias, y software relacionado incluye todas las actividades requeridas y/o necesarias para su correcta operación.

El IMSS en caso de contar con contratos de licenciamientos con distintos fabricantes (base de datos, sistema operativo o licenciamientos diversos), proporcionará a **KIO Networks** los datos requeridos para que **KIO Networks** a nombre del IMSS levante los tickets que en su caso se requieran a fin de solventar incidencias, eventos o actualizaciones.

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 del presente Anexo Técnico:

a) **KIO Networks** será responsable de la instalación, puesta a punto, gestión, administración, configuración, actualización, aplicación de parches y fixes 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) actualización de versiones y aplicación de parches y fixes. 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) **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.
i) 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.
j) **KIO Networks** instalará y proveerá las herramientas que le permitan automatizar las tareas de administración, generación, modificación, actualización de versiones, aplicación de parches y fixes 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 **KIO Networks**. En caso de requerir apoyo del fabricante, **KIO Networks** interactuará, escalar y coordinar con el fabricante, sí y sólo si, el producto tiene un defecto.
l) **KIO Networks** se apegará al mecanismo que el fabricante tenga definido para el levantamiento de un reporte, notificando al GGC del estado del reporte.
m) **KIO Networks** será responsable de levantar los casos de soporte directamente a los diferentes fabricantes de Base de Datos, sus componentes y/o subsistemas en caso de falla de producto, así como el seguimiento correspondiente. Así como de:

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) **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.
q) **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.
q) **KIO Networks** vigilará y mantendrá activas y vigentes las cuentas administrativas y operativas de Bases de Datos, 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) **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 y al Grupo de Control de Cambios, 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.
j) En caso de que el Instituto así lo determine como parte de su estrategia, **KIO Networks** entregará exportaciones, efectuar: cargas de información, migración o replicación de datos en las bases de datos como parte de los procesos de réplicas, migraciones, o configuraciones que el Instituto requiera para replicar o mover su información al centro de datos que se designe. incluyendo configuraciones, accesos, arquitecturas o lo que el Instituto determine sea requerido.

2.1.1.2.3 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 actualización de versiones, aplicación de parches y fixes, 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 menos una vez al mes 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 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, actualización de versiones, aplicación de parches y fixes 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) **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).

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. 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) **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** será responsable de levantar los casos de soporte directamente a los diferentes fabricantes de Base de Datos, sus componentes y/o subsistemas en caso de falla de producto, así como el seguimiento correspondiente. Así como de:

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

ANEXOS
DIVISIÓN DE CONTRATOS

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) **KIO Networks** 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, **KIO Networks** será responsable de la migración de Middleware a otro ambiente al que se encuentre actualmente ya sea en el Centro de Datos ofertado por **KIO Networks** o 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 incluyendo configuraciones, accesos, arquitecturas o lo que el Instituto determine sea requerido para las migraciones en comento,.

2.1.1.2.4 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 del presente Anexo Técnico.
b) **KIO Networks E** 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) **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** 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, **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.

2.1.1.2.5 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.

2.1.1.2.6 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 del presente Anexo Técnico y cuya implementación no afecte de forma negativa, genere conflicto, impida o limite las actividades que se espera que **KIO Networks** 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) o el sistema vigente acorde a la normatividad Institucional, **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

ANEXOS
DIVISIÓN DE CONTRATOS

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.

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** en caso de resultar adjudicado, 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, 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.

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 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) **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 deberán ser 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 éstas 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.

2.1.1.2.7 CONTROL DE 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 Grupo de Gobierno del Contrato 3 meses antes del vencimiento de las licencias.

KIO Networks entregará un informe mensual del tema de licenciamiento instalado por **KIO Networks**, detallando licenciamiento, versiones, aplicativo, arquitectura, correlaciones, dependencias e infraestructura donde se encuentra instalada.

- **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 deberá ser integrado en el mes que se haya actualizado y acordado con el Instituto.

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 Grupo de 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, Middleware y cualquier otro componente tecnológico utilizado por el Instituto.

KIO Networks 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.

KIO Networks entregará un informe mensual del tema de versionamiento instalado por **KIO Networks**, detallando versiones, aplicativo, arquitectura, correlaciones, dependencias e infraestructura donde se encuentra instalada.

2.1.1.2.8 AFINACIÓN (TUNING)

Con un enfoque proactivo, durante la vigencia del contrato 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 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.

KIO Networks será responsable de evaluar, analizar y corregir problemas de desempeño ocasionados por fallas del Sistema Operativo, Bases de Datos, 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.

ANEXOS
DIVISIÓN DE CONTRATOS

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.

KIO Networks entregará un informe mensual del tema de afinación (tuning) realizado por **KIO Networks**, detallando licenciamiento, versiones, aplicativo, arquitectura, correlaciones, dependencias e infraestructura donde se encuentra instalada.

2.1.1.2.9 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, de manera conjunta, EL INSTITUTO y **KIO Networks** realizarán un plan de trabajo con base en la línea base 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 a través del Grupo de Gobierno del Contrato para la optimización en la capacidad de procesamiento respecto de la línea base inicial, así como la optimización de licenciamiento, en aquellos equipos físicos que decida el cliente migrar a plataformas de virtualización o contenedores.

Adicionalmente, de manera conjunta, EL INSTITUTO y **KIO Networks** incluirán 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.

De manera conjunta, EL INSTITUTO y **KIO Networks** utilizarán las herramientas institucionales de virtualización o contenerización, así como una metodología de trabajo que 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 del Grupo 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 o contenedor, memoria virtual, clasificación (servidor web, servidor de aplicaciones, base de datos, etc.), software que utiliza el servidor virtual o contenedor, 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 ejecución de acuerdos, mecanismos, integraciones de participantes y demás elementos necesarios para las actividades de consolidación serán responsabilidad de **KIO Networks** previa aprobación de EL 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.

KIO Networks efectuará en conjunto con el IMSS, la migración anual a ambientes de contenedores de al menos el 33% de los aplicativos durante la vigencia del servicio.,.

2.1.1.2.10 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 durante de la vigencia del contrato, a fin de mantener las diferentes plataformas de licenciamiento (Sistema operativo, virtualizador, contenerizador, bases de datos, middleware, balanceadores, F5, actualizaciones, versiones, parches, hot fixes, entre otros), en las últimas versiones liberadas y probadas por el fabricante, para lo cual personal del IMSS deberá participar en el taller de trabajo a fin de evaluar y en su caso, realizar las adecuaciones al código de programación correspondiente.

KIO Networks entregará un informe mensual del tema de mantenimiento a plataformas, detallando características del licenciamiento, versiones, aplicativo, arquitectura, correlaciones, dependencias e infraestructura donde se encuentra instalada, vigencia de soporte técnico de cada una de las versiones, fin de soporte a las versiones por parte del fabricante, detalle de nuevas liberaciones por parte del fabricante y vulnerabilidades conocidas de las versiones instaladas, a fin de que de manera conjunta **KIO Networks** con el personal IMSS, efectúen las acciones correspondientes en caso de requerir adecuar código de programación o configuración, presentando a más tardar a mes vencido una propuesta de las plataformas a actualizar, consideraciones, riesgos y plan de trabajo para actualizarlas, a fin de que el equipo de trabajo IMSS participe en las acciones de actualización correspondientes, evitando la obsolescencia tecnológica de los licenciamientos y las vulnerabilidades (riesgos de seguridad) correspondientes.

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

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 o cualquier componente de HW y Software 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 deberá ser 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

ANEXOS
DIVISIÓN DE CONTRATOS

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 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.

El Instituto a través de sus áreas de desarrollo y negocio, proporcionará la autorización para la actualización de parches y *hotfixes*. En caso de que no existan condiciones para llevar a cabo dicha actualización, **KIO Networks** documentará en el control de cambios el riesgo de no aplicar estas recomendaciones.

KIO Networks entregará un informe mensual del tema de investigación y recomendaciones detallando recomendaciones por licenciamiento, versiones, aplicativo, arquitectura, correlaciones, dependencias e infraestructura donde se encuentra instalada, así como acciones a implementar para corregir la obsolescencia tecnológica y riesgos de seguridad inherentes.

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.

KIO Networks documentará correctamente los riesgos de la aplicación de cada parche. En caso de se detecte que el parche solicitara un reinicio, se debe de documentar correctamente la duración del reinicio en el control de cambios correspondiente a fin de EL INSTITUTO notifique a los usuarios de los servicios afectados para mitigar o anular cualquier impacto a la operación (ver la parte de ejecución).

a) **Ejecución**

Para los componentes, aplicativos y servicios de negocio en el alcance de este Anexo Técnico, **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 a la 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 del licitante y documentación contractual.

2.1.1.2.11 AUTOMATIZACIÓN DE COMANDOS

Como parte de la Administración de **KIO Networks** en los Sistemas Operativos, Bases de Datos, Middleware y componentes de software, **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.

KIO Networks entregará un informe mensual del tema de automatización de comandos detallando recomendaciones por licenciamiento, versiones, aplicativo, arquitectura, correlaciones, dependencias e infraestructura donde se encuentra instalada, así como acciones a implementar para automatización tecnológica, a fin de corregir la obsolescencia tecnológica y riesgos de seguridad inherentes.

Aspectos generales del apartado Gestión de Soporte a la Operación

KIO Networks ofertará, detallará, documentará, proporcionará, habilitará, configurará, pondrá a punto, operará y gestionará 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.

2.1.1.3 SOLUCIONES TECNOLÓGICAS PARA LA CONTINUIDAD OPERATIVA

2.1.1.3.1 VISIBILIDAD DE LOS SERVICIOS

KIO Networks en caso de resultar adjudicado, aprovisionará, implementará, configurará, pondrá a punto, operará, administrará, soportará y mantendrá todos los elementos de software, hardware y recursos humanos necesarios, como parte integral del servicio.

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 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 **KIO Networks** entregará un reporte técnico que lo sustente.

ANEXOS
DIVISIÓN DE CONTRATOS

Asimismo, en caso de que, por sus características, algún equipo no pueda ser monitoreado tomando en consideración las capas operativas solicitadas por el Instituto, **KIO Networks** entregará un reporte técnico acerca del alcance y características del monitoreo para estos equipos.
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,
5. Capa de base de datos,
6. Capa de virtualización, micro servicios y contenedores,
7. Indicadores de negocio,
8. Experiencia de usuario,
9. Correlación de eventos,
10. Interfases con entidades externas,
11. Capacity Planning que incluya tendencias de crecimiento y porcentaje de uso de la capacidad instalada,
12. Disponibilidad de los portales publicados en internet e intranet,
13. En su caso, ataques cibernéticos y su grado de afectación a los servicios.

KIO Networks entregará y explicará un informe mensual del tema de plan de capacidades que incluya el detalle de la infraestructura instalada, tendencias de crecimiento y porcentaje de uso de la capacidad instalada a fin de determinar posibles incrementos o decrementos de infraestructura por aplicativo, por tipo de infraestructura o plataforma incluyendo virtualizadores, contenedores y micro servicios, así como acciones a implementar para corregir las desviaciones detectadas, a fin de disminuir la obsolescencia tecnológica y riesgos de continuidad operativa y seguridad inherentes.

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 de **KIO Networks** cuente con elementos para identificar, aislar la causa raíz del evento y ejecute o sugiera acciones para su resolución.
d) **KIO Networks** entregará y explicará un informe mensual del tema de correlación de eventos que incluya el detalle de la infraestructura instalada, a fin de determinar posibles mejoras continuas de infraestructura por aplicativo, por tipo de infraestructura o plataforma incluyendo virtualizadores, contenedores y micro servicios, así como acciones a implementar para corregir las desviaciones detectadas, a fin de disminuir la obsolescencia tecnológica y riesgos de continuidad operativa y seguridad inherentes.
e) El acceso para administración deberá ser mediante interfaz Web a una consola centralizada desde cualquier punto de la red del Instituto.
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.

KIO Networks entregará y explicará un informe mensual del tema de análisis en detalle o drill down desde los mapas que incluya el detalle de la infraestructura instalada, por aplicativo, por tipo de infraestructura o plataforma incluyendo virtualizadores, contenedores y micro servicios, así como acciones a implementar para corregir las áreas de mejora continua o desviaciones detectadas, a fin de disminuir la obsolescencia tecnológica y riesgos de continuidad operativa y seguridad inherentes.

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 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 tendrá 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 solución deberá tener habilitada y en operación la funcionalidad 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 y autorizados por el IMSS**.

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, 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 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 del presente anexo técnico, 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.

KIO Networks entregará y explicará un informe mensual del tema de distintas vistas de la salud, estado y desempeño de los BCF, que incluya el detalle de la infraestructura instalada, infraestructura por aplicativo, por tipo de infraestructura o plataforma incluyendo virtualizadores, contenedores y micro servicios, así como acciones a implementar para corregir las áreas de mejora continua o desviaciones detectadas, a fin de disminuir la obsolescencia tecnológica y riesgos de continuidad operativa y seguridad inherentes.

KIO Networks habilitará accesos a su herramienta de monitoreo al personal designado por el IMSS, de la misma manera, **KIO Networks** habilitará una réplica de la base de datos de monitoreo en las instalaciones designadas por

ANEXOS
DIVISIÓN DE CONTRATOS

el IMSS a efecto de que el IMSS pueda estar visualizando el estado de los servicios y los eventos de monitoreo de manera en línea.

KIO Networks entregará y explicará al menos mensualmente un reporte del análisis de uso de recursos a efecto de dimensionar el right sizing, esto es, incrementar sus capacidades por posible incremento del consumo respecto a lo estimado, corroborar que están en un nivel de uso adecuado o en su caso, disminución de capacidades por haber decaído su consumo respecto del estimado, posible reasignación de recursos, así como su posible manejo como recursos compartidos.
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.
KIO Networks efectuará y explicará al menos mensualmente un reporte del desarrollo e implementación de las vistas de las aplicaciones y servicios que hoy se encuentran desplegadas en el Centro de Datos actual, a fin de analizar el uso de infraestructura y métricas de negocio de cada aplicativo en comento.
y) **KIO Networks** implementará y operará 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.
KIO Networks entregará y explicará un informe mensual del tema experiencia de usuario, que incluya el detalle de la infraestructura instalada, infraestructura por aplicativo, por tipo de infraestructura o plataforma incluyendo virtualizadores, contenedores y micro servicios.
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 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.

Adicionalmente **KIO Networks** habilitará monitoreo de la operación de los servicios y aplicativos que operan en la infraestructura tecnológica ofertada, incluyendo métricas de negocio de los aplicativos correspondientes.

Análisis de flujos de tráfico

KIO Networks realizará 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 **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 entregará y explicará al IMSS un informe mensual del tema de análisis de flujos de tráfico, que incluya el detalle de la infraestructura instalada, infraestructura por aplicativo, por tipo de infraestructura o plataforma incluyendo virtualizadores, contenedores y micro servicios.

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 deberá ser suministrada, instalada, configurada, implementada, soportada, puesta a punto y operada por **KIO Networks**. Es responsabilidad de **KIO Networks** mantener actualizada las versiones, parches y configuraciones para la correcta operación de la solución, en caso de que para la actualización se requiera participación del personal IMSS, **KIO Networks** manifestará expresamente la necesidad de la participación de la gente IMSS, el alcance, así como un plan de trabajo para que de manera conjunta **KIO Networks** e IMSS logren la actualización de versiones, parches y configuraciones para la correcta operación.

KIO Networks entregará y explicará al IMSS un informe mensual de la solución que incluya todo el hardware, software y personal necesarios para la entrega del servicio, la cual deberá ser suministrada, instalada, configurada, implementada, soportada, puesta a punto y operada por **KIO Networks**. Es responsabilidad de **KIO Networks** mantener actualizada las versiones, parches y configuraciones para la correcta operación de la solución, que incluya el detalle de la infraestructura instalada, infraestructura por aplicativo, por tipo de infraestructura o plataforma incluyendo virtualizadores, contenedores y micro servicios.

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:
   a. Tráfico por país,
   b. Tráfico por región,
   c. Tráfico por ciudad
   d. Tráfico por aplicativo

e) Generación y entrega de reportes en tiempo real y en forma programada de eventos que incluyen anomalías clasificadas por niveles de severidad configurables.
   a. Tráfico por país,
   b. Tráfico por región,
   c. Tráfico por ciudad

ANEXOS
DIVISIÓN DE CONTRATOS

d. Tráfico por aplicativo

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 de manera enunciativa más no limitativa, 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 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.

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 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 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.

ANEXOS
DIVISIÓN DE CONTRATOS

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 las 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 una 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.

2.1.1.3.2 SOPORTE

Será responsabilidad de **KIO Networks** incluirá 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.

2.1.1.3.3 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 de **KIO Networks** 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** en caso de resultar ganador 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.

<<Integración de CMDB de Proveedor actual>>

KIO Networks designará un **coordinador de configuraciones**, quien deberá tener 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.

Mensualmente, el licitante deberá entregar de manera actualizada en medios ópticos o electrónicos copia de la CMDB a la CIT y a la CSITI, como parte de su documentación para trámite a pago de los servicios, incluyendo el detalle de la facturación mensual por BCF y acumulada en la vigencia del contrato.

Aspectos generales del apartado Soluciones Tecnológicas del Centro de Continuidad Operativa

KIO Networks en caso de resultar adjudicado, ofertará, detallará, documentará, proporcionará, habilitará, configurará, pondrá a punto, operará y gestionará 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.

2.1.1.4 CONTRAPRESTACIÓN DEL SERVICIO

El servicio de **Continuidad a la Operación y Soporte** será devengado y de manera mensual se realizará el trámite de pago previa aceptación del servicio por el Grupo de Administración del Contrato.

La documentación probatoria correspondiente deberá ser entregada en medio electrónico (repositorio y DVD).

2.1.2 Consumo de BCFs para el Servicio

El servicio **Continuidad a la Operación y Soporte** permitirá el consumo de todos los BCFs en modalidad de despliegue Centro de Datos Primario; igualmente se encargará del despliegue de aquellos BCFs que correspondan a sus funciones en las modalidades de despliegue Extensión de Nube Privada (ENP) en los puntos con mayor demanda transaccional de operación de los servicios del Instituto" y "Servicios desplegados en Instalaciones designadas por el Instituto".

KIO Networks entregará de manera mensual el **Informe de Consumo y Disponibilidad de los BCFs** que soporte las acciones referentes a este apartado.

2.1.3 Plataformas para el Servicio de Continuidad a la Operación y Soporte

2.1.3.4 PLATAFORMA DE VIRTUALIZACIÓN Y CONTENERIZACIÓN EN LAS DIFERENTES MODALIDADES

a) **KIO Networks** suministrará una plataforma de virtualización y contenerizacion que soporte las diferentes tecnologías de sistema operativo en la modalidad de despliegue CDP, ENP, SDI.
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.

ANEXOS
DIVISIÓN DE CONTRATOS

c) Debe soportar la creación y administración de máquinas virtuales o contenedores, 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 y contenerización solicitados para las tecnologías que tenga establecidas el Marco Tecnológico de Referencia del Instituto.
Actividades que deberá realizar **KIO Networks** como parte del servicio de plataforma de virtualización y contenerización:
a) Instalación, Configuración, puesta a punto y administración de la consola de administración para la plataforma de virtualización y contenerización.
b) Creación de nuevas máquinas virtuales y contenerización que se necesiten por nuevas necesidades del Instituto.
c) Configurar la solución de virtualización y contenerización a efecto de proporcionar de manera temporal, dinámica y sin afectar ninguna de las máquinas virtuales y contenerización 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 y contenerización 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 y contenerización a otros nodos activos.
e) Configurar la solución de virtualización y contenerización a efecto de mantener un balanceo dinámico de los recursos de hardware asignados a una o más de las máquinas virtuales y contenerización del Instituto, relocalizando máquinas virtuales y contenerización en nodos con menor carga de trabajo sin sufrir afectación de ninguna clase en las mismas.
f) Configurar la solución de virtualización y contenerización 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 y contenerización del Instituto en uno o más nodos activos.
g) Configurar la solución de virtualización y contenerización para mover máquinas virtuales y contenerización 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 y contenerización entre máquinas físicas en línea y sin interrupción en la disponibilidad de las aplicaciones y servicios que residen sobre las máquinas virtuales y contenerización.
h) El software de Virtualización y contenerización 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 y contenerización a efecto de realizar la virtualización de equipos físicos o la conversión de máquinas virtuales y contenerización en formatos de una plataforma de virtualización a otra.
j) Configurar la solución de virtualización y contenerización a efecto de realizar la instalación y actualización al software de virtualización y contenerización, 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 y contenerización.
k) Configurar la solución de virtualización y contenerización a efecto de crear mensualmente, sin caer en interrupciones del servicio, imágenes de máquinas virtuales y contenerización activas o inactivas a manera de respaldo o con el fin de mantener máquinas virtuales y contenerización para probar actualizaciones o parches permitiendo analizar el comportamiento del sistema operativo o sus aplicaciones.

2.1.4 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.

2.1.5 Servicios extendidos

Conforme a lo que se señalará más adelante, los servicios extendidos se conceptualizan en el presente documento para prever situaciones que derivado de la complejidad de la arquitectura con la cual se ha construido el ecosistema del Instituto se haga necesario activarlo bajo reglas específicas que atiendan el marco normativo vigente legal y técnico que deben observar para coadyuvar al logro y las Metas y Objetivos Institucionales

En su caso **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 que llegaran a requerirse.

2.1.6 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 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.

.

2.2 Servicios de Continuidad y Soporte de Telecomunicaciones

2.2.1 Plataformas de Servicios de Telecomunicaciones

2.2.1.1 Punto Neutro

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

ANEXOS
DIVISIÓN DE CONTRATOS

- 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 **KIO Networks** 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.

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.

2.2.1.1.1 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.

2.2.1.1.1.1 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 en caso de resultar adjudicado, brindara 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.

ANEXOS
DIVISIÓN DE CONTRATOS

- 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.

2.2.1.1.1.2 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.

2.2.1.1.1.3 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.

2.2.1.1.1.4 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 cubrirá 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 volumen 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.

2.2.1.1.1.5 UNIDAD DE CONECTIVIDAD DE INTERNET. (UCI).

KIO Networks proveerá conectividad hacia los servicios web nacionales y mundiales.

KIO Networks 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.

KIO Networks 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.

2.2.1.1.1.6 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.

2.2.1.1.2 COMUNICACIONES

2.2.1.1.2.1 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.

2.2.1.1.2.2. 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 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.

2.2.1.2 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.

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.
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.

2.2.1.2.1 INFRAESTRUCTURA E INSTALACIONES

KIO Networks facilitará 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,

AUTOS
DIVISIÓN DE CONTRATOS

- 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. **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** 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 **KIO Networks** 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.

2.2.1.2.2 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 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

2.2.1.2.3 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** 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 **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.

ANEXOS
DIVISIÓN DE CONTRATOS

- 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 **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.

2.2.1.2.4 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.
- 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 **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 ENP 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 deberá garantizar la capacidad de integración de dispositivos diferentes a PAN usando dicha identidad.

2.2.1.2.5 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 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 **KIO Networks** hará una propuesta para este servicio. Para cada integración **KIO Networks** presentará un plan de trabajo que deberá ser aprobado por el Instituto.

2.2.1.2.6 FUNCIONALIDADES GENERALES DEL SERVICIO

KIO Networks proporcionará 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.

2.2.1.2.7 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.

2.2.2 Servicios eventuales

A lo largo del **Servicio de Operación y Soporte de 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.

2.2.3 Servicios extendidos

Conforme a lo que se señalará más adelante, los servicios extendidos se conceptualizan en el presente documento para prever situaciones que derivado de la complejidad de la arquitectura con la cual se ha construido el ecosistema del Instituto se haga necesario activarlo bajo reglas específicas que atiendan el marco normativo vigente legal y técnico que deben observar para coadyuvar al logro y las Metas y Objetivos Institucionales

En su caso **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 que llegaran a requerirse.

2.3 Servicio de Continuidad y Soporte de Seguridad

2.3.1 Soporte para la Operación de la Seguridad de la Nube IMSS

2.3.1.1 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 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, 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 24 horas 7 días de cada semana durante la vigencia del servicio.
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

ANEXOS
DIVISIÓN DE CONTRATOS

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 Servicio de Operación y Calidad de la Seguridad informática perimetral

2.3.1.2 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.

2.3.1.2.1 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. La infraestructura propuesta deberá ser de última generación, dedicada y que permita la segmentación del tráfico para ambiente públicos y privados de manera independiente; exclusivamente para las necesidades del Instituto y **KIO Networks** cumplirá 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.
Segmentación de tráfico de ambientes públicos y privados de manera independiente en equipos de propósito específico, apegándose a las especificaciones en el Apéndice 5 para la clasificación de Firewall para Enlaces de Banda Ancha mayor a 100Mbps y hasta 1Gbps.

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, **KIO Networks** realizará la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades.

2.3.1.2.2 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).
La solución propuesta por el licitante deberá estar listada como líder en el Cuadrante de Gartner
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.

ANEXOS
DIVISIÓN DE CONTRATOS

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.

2.3.1.2.3 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:
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 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 por el fabricante.
Garantizar la disponibilidad del servicio solicitada por EL INSTITUTO propuesto por **KIO Networks.**
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 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.

2.3.1.2.4 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:
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.
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.

2.3.1.2.5 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.
Garantizar la disponibilidad del servicio solicitada por EL INSTITUTO propuesto por **KIO Networks**.
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.

ANEXOS
DIVISIÓN DE CONTRATOS

KIO Networks integrará la solución a su consola de administración
Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada por 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.

Firewall Especializado en Servicios de Base de Datos

Descripción del servicio:
El Instituto requiere de una solución de protección para bases de datos, que permita brindar: la protección a los servidores de bases de datos en tiempo real, el monitoreo del tráfico de base de datos que fluye a través de la red del Instituto o bien de forma local, la detección de ataques avanzados sobre las instancias y sus bases de datos.

Detalles del Servicio:
Definir en conjunto con el Instituto la estrategia de habilitación de la solución de Firewalls de base de datos en la arquitectura de seguridad y comunicaciones.
Llevar a cabo todas las tareas necesarias para la revisión de los equipos de acuerdo a su arquitectura 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 la solución que integran el servicio sin un control de cambios autorizado por este último.
Integrar cada dispositivo hacia su respectiva consola de administración.
No utilizar la auditoria nativa del manejador de bases de datos para su correcto y completo funcionamiento.

Ser compatible con los manejadores de bases de datos del Instituto;
Monitorear y auditar todas las operaciones de las bases de datos en tiempo real para conocer el detalle de quién, qué, cuándo, dónde y cómo se realizó todas y cada una de las transacciones en las bases de datos;
Monitorear y auditar todos los accesos a las bases de datos. Es decir, todas las consultas que se realicen a las bases de datos desde los diferentes clientes y/o aplicaciones, o directamente conectados al servidor de las bases de datos, logrando que el Instituto tenga la visibilidad completa de todos los accesos y consultas SQL;
Monitorear respuestas de la base de datos;
Detectar y bloquear transacciones SQL no autorizadas, ya sea el acceso desde un aplicativo, usuario privilegiado en la red o en el mismo servidor de base de datos;

Lo anterior deberá ser manejado desde políticas predefinidas y personalizables;
Detectar y bloquear intentos de explotar vulnerabilidades descubiertas;
Detectar y bloquear actividad sospechosa encontrada en las bases de datos;
Permitir acciones inmediatas de bloqueo, generación de alertas, envío de alertas de transacciones no autorizadas en las bases de datos.

2.3.1.3 ENTREGABLES DE ÚNICA OCASIÓN

2.3.1.3.1 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 Monitoreo de Eventos
  - Proceso de Análisis
  - Proceso de Contención de Incidentes
  - Proceso de Escalamiento
  - Proceso de Atención a Fallas
  - Proceso de Liberación de Servicios a Operación
  - Proceso de Ejecución de Cambios
- 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

2.3.1.4 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

2.3.1.4.1 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.

ANEXOS
DIVISIÓN DE CONTRATOS

- 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.

2.3.1.4.2 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.

2.3.1.4.3 ANTI-DENEGACIÓN DE SERVICIOS (DDOS)

- Reporte de inspección de tráfico del servicio DDoS
- Reporte de los controles de cambios en el servicio de DDoS
- Reporte de incidentes atendidos en el servicio de DDoS
- Reporte de fallas atendidas en el servicio de DDoS
- Reporte del top diez (10) de portales con más ataques bloqueados (DDoS)
- Reporte de Alertas DDoS
- Reporte del top de violaciones
- Reporte de eventos e incidente

2.3.1.4.4 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.

2.3.1.4.5 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.

2.3.1.4.6 CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

- Reporte de los requerimientos de cambios registrados (ABC) a través de la Mesa de Servicios (SOC)
- Reporte de los registros de incidentes reportados y atendidos a través de la Mesa de Servicios (SOC)
- Reporte de nivel de servicio: Entrega del Servicio
- Reporte de nivel de servicio: Disponibilidad
- Reporte de nivel de servicio: Desempeño
- Reporte de nivel de servicio: Impacto a la Operación
- Reporte de nivel de servicio: Atención de Solicitudes
- Reporte de Nivel de Servicio - Reportes de Administración por procesos, incidentes y problemas
- Reporte de Nivel de Servicio - Reportes de Administración por procesos: Administración de configuraciones
- Reportes de Nivel de Servicio - Reporte de Administración por procesos: Administración de cambios
- Reporte de Nivel de Servicio - Reporte de Administración por procesos: Administración de problemas
- Reporte de utilización y desempeño
- Entregable Mensual del Servicio de Administración y Soporte de Componentes de Seguridad
- Entregable Mensual del Servicio de Centro de Operaciones de Seguridad

2.3.1.5 ENTREGABLES BAJO DEMANDA

KIO Networks generará bajo demanda los siguientes documentos y/o reportes, a solicitud del Servicio de Operación y Calidad de la Seguridad Informática Perimetral; y que incluyen de manera enunciativa más no limitativa los siguientes conceptos:

2.3.1.5.1.1 SERVICIOS DE OPERACIÓN

- Reportes bajo demanda de los servicios de operación que puedan ser extraídos de cada solución que se encuentre operativa.

ANEXOS
DIVISIÓN DE CONTRATOS

2.3.1.6 CONSIDERACIONES GENERALES PARA LA ENTREGA DE LOS SERVICIOS DE SEGURIDAD

KIO Networks en caso de resultar adjudicado, 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 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, para lo cual, **KIO Networks** presentará al personal designado por el Instituto, un plan de trabajo en el que se consideren todas las actividades, tareas rollback y tiempos por cada uno de dichos elementos, de tal forma que se tenga el tiempo estimado y si tendrá o no impacto en la operación.

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 y deberá hacer una integración con la Mesa de Servicios Tecnológicos del Instituto.

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.

Proporcionar acceso de lectura a las Consolas de las soluciones de Seguridad al personal responsable del Instituto, el cual será determinado por el Administrador del Contrato.

KIO Networks generará un Dashboard ejecutivo en el cual se deberá presentar información relativa a las tendencias de seguridad, disponibilidad y alertas de seguridad.

2.3.2 Servicios eventuales de seguridad

A lo largo del Servicio de Continuidad y Soporte de Seguridad, se señalan una serie de servicios que pueden ser consumidos de manera eventual.

2.3.3 Servicios extendidos

Conforme a lo que se señalará más adelante, los servicios extendidos se conceptualizan en el presente documento para prever situaciones que derivado de la complejidad de la arquitectura con la cual se ha construido el ecosistema del Instituto se haga necesario activarlo bajo reglas específicas que atiendan el marco normativo vigente legal y técnico que deben observar para coadyuvar al logro y las Metas y Objetivos Institucionales

En su caso **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 que llegaran a requerirse.

2.4 Servicio de Gestión de Medición del Desempeño de Aplicativos y Componentes Institucionales

KIO Networks incluirá en la 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.

KIO Networks incluirá en la 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** en caso de resultar adjudicado o en otro Centro de Datos que el Instituto designe para las pruebas.

KIO Networks incluirá en la 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.

ANEXOS
DIVISIÓN DE CONTRATOS

KIO Networks ofertará, detallará y describirá en su propuesta que el servicio requerido por el Instituto incluirá por lo menos los siguientes elementos:

2.4.1 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 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.
- **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.

2.4.2 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** determinará 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** incluirá en la 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** incluirá en la 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.

2.4.3 De la fase de propuesta para su implementación en un estado mínimo funcional:

- **KIO Networks** incluirá en la propuesta, que, considerando el resultado de la fase anterior, deberá presentar una propuesta para la reducción del ecosistema del aplicativo o componente Institucional seleccionado.
- **KIO Networks** en caso de resultar adjudicado 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** en caso de resultar adjudicado 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.

ANEXOS
DIVISIÓN DE CONTRATOS

- 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.

2.5 Migración del Centro de Datos Actual al Centro de Datos Ofertado por el KIO Networks (en caso de aplicar)

KIO Networks ofertará en caso de que aplique el servicio de Migración desde el Centro de Datos actual hacia el Centro de Datos ofertado, el cual deberá incluir el proceso de migración de aplicaciones, servicios, infraestructura de procesamiento, almacenamiento, respaldo, seguridad y telecomunicaciones, incluyendo procedimientos, esquemas, tecnologías, herramientas y perfil del personal para ejecutar la migración, que de manera enunciativa más no limitativa deberá integrar las siguientes opciones:

- Migración de aplicación o servicios incluyendo instalación, configuración, puesta a punto de componentes, aplicaciones, bases de datos, middleware o lo necesario para efectuar el servicio de migración.
- Exportación/Importación de máquinas virtuales a través de formatos estándares a la plataforma ofertada por **KIO Networks** que permitan poder importar, configurar, poner a punto y validar las diferentes maquinas migradas al centro de datos ofertado.
- Migración de virtualizador a virtualizador con software que permita el movimiento de máquinas entre los virtualizadores actuales y ofertado, incluyendo el software o la plataforma que permita el movimiento, copia, importación, despliegue de máquinas virtuales.
- Migración de infraestructura de almacenamiento y respaldos, usando esquemas de replicación de información o mecanismos que permitan replicar la información en el centro de datos ofertado.
- en su caso, **KIO Networks** podrá proponer herramientas o mecanismos adicionales para la migración la cuales deberán ser evaluados y aprobados por el Instituto.

Las opciones propuestas por **KIO Networks** serán analizadas, entre el Instituto y **KIO Networks** en las mesas de trabajo de seguimiento semanal y podrán ser modificadas, de acuerdo a la criticidad, impacto y complejidad de cada aplicación, componente, servicio o infraestructura así como disponibilidad de los prerrequisitos en cada caso.

La(s) opcion(es) utilizada(s) por **KIO Networks**, deberá(n) de ejecutarse en los horarios establecidos por el Instituto, los cuales serán establecidos y modificados en las reuniones de seguimiento semanal.

El criterio para considerar concluida la migración desde el Centro de Datos actual hacia el Centro de Datos ofertado, será en el momento en que se encuentren los servicios descritos anteriormente activos y operando en la infraestructura propuesta por el Licitante, e interactuando con el ecosistema tecnológico institucional, esto es; con los ambientes operativos digitales productivos y no productivos instalados en los diferentes centros de datos IMSS y del Gobierno Federal así como organismos con los que interactúa el Instituto tales como SAT, RENAPO, INFONAVIT, BANCO DE MÉXICO, PROCESAR, CONSAR, BANCOS Y AFORES, entre otros, validados de conformidad por el personal que el Instituto designe (áreas de telecomunicaciones y seguridad informática,

infraestructura tecnológica, desarrollo, monitoreo así como el personal de las direcciones normativas que hacen uso de los servicios en los casos que aplique).

En el **Apéndice "Descripción Detallada de los Servicios de Continuidad de Nube IMSS"** se encuentra el detalle de los componentes para la Migración del Centro de Datos Actual al Centro de Datos Ofertado por **KIO Networks**:

- Migración de Infraestructura de procesamiento, almacenamiento, respaldo, telecomunicaciones y seguridad.
- Migración de Aplicativos, componentes y Servicios del Instituto al Centro de Datos Ofertado por **KIO Networks**.

La relación de servicios y aplicativos a migrar por **KIO Networks** se encuentra en el Apéndice 3 denominado **"Listado de aplicaciones"** y durante la ejecución de la migración, **KIO Networks en caso de aplicar** garantizará:

- La continuidad de los servicios que el Instituto presta a derechohabientes, patrones, pensionados, trabajadores del Instituto y público en general,
- La interoperabilidad dentro del ecosistema de infraestructura tecnológica del Centro de Datos ofertado por **KIO Networks** con los Centros de Datos Institucionales ubicados en Monterrey, Cd. De México y Guadalajara, Centros de Datos del Gobierno Federal ubicados en San Luis Potosí, así como cualquier otro centro de datos definido por el Instituto.
- La interoperabilidad con los inmuebles Institucionales a nivel nacional.
- La publicación de aplicaciones y servicios digitales Institucionales a través de Internet.
- La comunicación con los ecosistemas de infraestructura tecnológica de entidades externas con los que el IMSS interopera tales como: SAT, RENAPO, Procesar, Banco de México, INFONAVIT, Bancos, Instituto Nacional Electoral, Afores, CONSAR, entre otros.

Al concluir cualquier actividad de migración validada y aprobada por el Instituto, **KIO Networks** entregará al Instituto, memoria(s) técnica(s) de la(s) migración(es) realizada(s), la cual entre otras cosas deberá incluir de manera enunciativa más no limitativa: configuraciones de infraestructura, aplicaciones, componentes, software, middleware, bases de datos, entre otros incluyendo lo necesario para su operación.

KIO Networks ofertará en la propuesta económica (en caso de aplicar) el costo del concepto de migración bajo el rubro "migración de centros de datos", incluyendo los procesos de migración de información, aplicativos, sistemas y servicios electrónicos o digitales del IMSS e infraestructura del Centro del Datos Actual a la infraestructura ofertada por **KIO Networks**, así como los procesos de migración de infraestructura de telecomunicaciones y seguridad que permita:

- La interoperabilidad dentro del ecosistema de infraestructura tecnológica del Centro de Datos ofertado por **KIO Networks** con los Centros de Datos Institucionales ubicados en Monterrey, Cd. De México y Guadalajara, Centros de Datos del Gobierno Federal ubicados en San Luis Potosí, así como cualquier otro centro de datos definido por el Instituto.
- La interoperabilidad con los inmuebles Institucionales a nivel nacional.
- La publicación de aplicaciones y servicios digitales Institucionales a través de Internet.
- La comunicación con los ecosistemas de infraestructura tecnológica de entidades externas con los que el IMSS interopera tales como: SAT, RENAPO, Procesar, Banco de México, INFONAVIT, Bancos, Instituto Nacional Electoral, Afores, CONSAR, entre otros.

Al concluir cualquier actividad de migración del "Punto Neutro" validada y aprobada por el Instituto, **KIO Networks** entregará al Instituto, memoria(s) técnica(s) de la(s) migración(es) realizada(s), la cual entre otras cosas deberá incluir de manera enunciativa más no limitativa: configuraciones de infraestructura, componentes, software, entre otros incluyendo lo necesario para su operación.

Al concluir cualquier actividad de migración del centro de datos móvil, validada y aprobada por el Instituto, **KIO Networks** entregará al Instituto, memoria(s) técnica(s) de la(s) migración(es) realizada(s), la cual entre otras cosas

ANEXOS
DIVISIÓN DE CONTRATOS

deberá incluir de manera enunciativa más no limitativa: configuraciones de infraestructura, aplicaciones, componentes, software, middleware, bases de datos, entre otros incluyendo lo necesario para su operación.

KIO Networks realizará las actividades correspondientes para garantizar la operación del servicio migrado y operar la infraestructura, aplicaciones y servicios en cualquiera de las modalidades descritas en el presente anexo técnico, garantizando los niveles de servicio (99.982% de disponibilidad en toda la solución ofertada durante la vigencia del contrato) señalados en el apartado **"Niveles de Servicio"** a fin de brindar continuidad a los procesos de negocio internos y externos al IMSS.

2.6 Elementos comunes de los servicios

2.6.1 Servicio de Infraestructura y Bloques de Construcción Fundamentales.

KIO Networks en caso de resultar adjudicado, aprovisionará cualquiera de los componentes de infraestructura establecidos en el apéndice 1 de "Componentes de Infraestructura" 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
    - 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 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 proporcionan el esquema de categorización para describir cómo y/o donde un BCF 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. "Componentes de Infraestructura". 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.

ANEXOS
DIVISIÓN DE CONTRATOS

2.6.2 UNIDADES DE SOPORTE EXTENDIDO

2.6.3 Servicio de Soporte Extendido para el Centro de Cómputo

El Servicio de Soporte Extendido se contratará bajo demanda y se ejercerá a partir de Unidades de Soporte Extendido, siendo necesario la existencia de una solicitud de servicio por parte del Administrador del Contrato que recibirá un tratamiento individual por parte de **KIO Networks**.

2.6.4 Descripción del Servicio

El monto máximo a ejercer por medio de las Unidades de Soporte Extendido será máximo del 10% del valor total de la cotización económica del proveedor.
El valor de la Unidad de Soporte Extendido se calculará dividiendo el monto de la propuesta de **KIO Networks** del servicio de soporte extendido entre el monto máximo determinado por el 10% del valor total de la cotización económica de **KIO Networks**.

Los servicios que estarán a cargo del proveedor para cada una de las Unidades de Soporte Extendido serán los necesarios para cumplir con los objetivos y alcance del Proyecto-Servicio.

Los servicios o proyectos solicitados a través de estas figuras 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 se efectúe a través del Administrador del Contrato, **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:

1. Objetivos del Proyecto-Servicio.
2. Alcances del Proyecto-Servicio.
3. Actividades a realizar (Plan de Trabajo Detallado) que incluya fechas compromiso para los entregables.
4. En su caso, desglose técnico de los componentes que integren el servicio a prestar.
5. Justificación técnica de la correspondencia del objetivo del proyecto-servicio con las Unidades de Soporte Extendido.

Los costos unitarios de estos servicios se derivan de la cotización económica de **KIO Networks.**

2.6.5 Mecanismo de consumo de las Unidades de Soporte Extendido

Las Unidades de Soporte Extendido se consumirán sólo a través de Proyectos-Servicios que resultarán del desarrollo de una justificación técnica, misma que podrá estar relacionada de manera enunciativa más no limitativa con los servicios del presente Anexo Técnico o el objeto del contrato, entre ellos:

1. Análisis de incorporación de servicios no previstos en este Anexo Técnico.
2. Análisis de incorporación/integración de servicios administrados de almacenamiento, explotación de datos, procesamiento, seguridad, comunicaciones, software, pertenecientes a dominios complementarios al presente anexo técnico, como, por ejemplo:
   - Servicio de autenticación de usuarios
   - Servicio de mensajería de colas
   - Servicio de caché
   - Servicio de balanceo
   - Servicio de consola de administración
   - Servicio de notificaciones
   - Servicio de certificaciones
   - Servicio de aprovisionamiento de nombres de Dominio
   - Migración de base de datos
   - Servicio administrado de DataWareHouse
   - Servicio administrado de BI

3. Labores específicas de apoyo al Grupo Administrador del Contrato en procesos no definidos en este Anexo Técnico.
4. 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.
5. Trabajos tendientes a la homogenización de servicios TIC, dentro de los cuales pudiera incluirse la provisión de servicios administrados.
6. Análisis y solución de incidencias / problemas de la infraestructura habilitadora para procesos no definidos.
7. Análisis y solución de incidencias / problemas de la infraestructura donde convergen las soluciones provistas por el servicio objeto del presente Anexo Técnico.
8. Análisis y solución de incidencias / problemas de la infraestructura de distribución, procesamiento, almacenamiento, seguridad, comunicaciones y software donde convergen las soluciones provistas por el servicio objeto del presente Anexo Técnico.
9. Análisis y solución de incidencias / problemas de la infraestructura de transición, migración u operación de redes, soluciones, sistemas, portales, front y backend de sistemas de la Institución.

2.6.6 Modalidad de Proyecto y Servicio de Soporte Extendido

Cada servicio deberá recibir un tratamiento individual por parte de **KIO Networks**, lo cual incluye asignar a un **Coordinador de Proyecto de Soporte Extendido** por solicitud, quien será responsable del mismo. Dicho coordinador deberá asistir a las reuniones requeridas por la Institución para determinar el alcance del proyecto, así como dar el seguimiento al mismo hasta su conclusión

3 FIRMAS DE ELABORACION, REVISION Y APROBACION

Atentamente

DocuSigned by:
413DA358D32D4B3...

JUAN CARLOS MARTÍNEZ VALDÉS
REPRESENTANTE LEGAL
SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.

SIN TEXTO

DocuSign Envelope ID: 658B6DB9-3AF3-424C-8656-941FE346D1BF

Términos y Condiciones

SGMP_Términos y Condiciones

Coordinación de Servicios de Infraestructura Tecnológica Institucional

KIO Networks

Servicio de Continuidad de la Nube IMSS 2022

Ciudad de México a 13 de abril de 2022

Esta información es propiedad de Sixsigma Networks México, S.A. de C.V. (KIO NETWORKS), se proporciona con el carácter de confidencial. Esta información no será reproducida, usada o divulgada total o parcialmente por cualquier razón diferente que la de evaluar la propuesta de Servicios de KIO NETWORKS.

ANEXOS
DIVISIÓN DE CONTRATOS

ÍNDICE

1 OBJETIVO DEL DOCUMENTO 3
2 ALCANCE DEL SERVICIO 3
3 REQUERIMIENTOS TECNICOS 4
4 PLAZO DE LOS SERVICIOS 5
5 PERFIL DEL PROVEEDOR 5
6 CUMPLIMIENTO DE OBLIGACIONES CONTRACTUALES 8
7 CLAUSULAS Y CUMPLIMIENTOS 8
8 ADMINISTRADORES DEL CONTRATO 10
9 DERECHOS DE AUTOR 10
10 CONFIDENCIALIDAD 11
11 CONFORMACION DE LA PROPUESTA 12
12 GARANTIAS 15
13 NIVELES DE SERVICIO 15
14 PENAS CONVENCIONALES Y DEDUCTIVAS 16
15 ACUERDOS DE NIVELES OPERACIONALES 16
16 UBICACIONES PARA LA PRESTACION DEL SERVICIO 17
17 CONSIDERACIONES PARA LA FINALIZACION DEL CONTRATO 17
18 PAGO DE LOS SERVICIOS 17
19 MECANISMOS DE CONTROL PARA LA ADMINISTRACION 20
20 CRITERIO DE EVALUACION 21
21 LICENCIAS, PERMISOS, REGISTROS, CETIFICADOS O AUTORIZACIONES QUE DEBE CUMPLIR O APLCIARSE AL BIEN O SERVICIO A CONTRATAR 32
22 FOLETOS, CATALOGOS, FOTOGRAFIAS, MANUALES ENTRE OTROS, EN CASO DE QUE SE REQUIERAN PARA COMPROBAR LAS ESPECIFICACIONES TECNICAS REQUERIDAS 33
23 VISITAS A LAS INSTALACIONES INSTITUCIONALES, DONDE SE SUMINISTRARAN O COLOCARAN LOS BIENES O DONDE SE PRESTARAN LOS SERVICIOS, EN SU CASO 33
24 EN SU CASO, MECANISMOS REQUERIDOS AL PROVEEDOR PARA RESPONDER POR DEFECTOS O VICIOS OCULTOS DE LOS BIENES O DE LA CALIDAD DE LOS SERVICIOS 33
25 RESPONSABILIDAD 33
26 RESPONSABILIDAD LABORAL 33
27 FIRMAS DE ELABORACION, REVISION Y APROBACION 34

KIO Networks

DS JCHV DS JAR

1 OBJETIVO DEL DOCUMENTO

Definir a **Sixsigma Networks S.A. de C.V.** en lo consecutivo **KIO Networks** los términos y condiciones del **Servicio de Continuidad de la Nube IMSS 2022.**

2 ALCANCE DEL SERVICIO

KIO Networks, brindará continuidad operativa, soporte, gestión de la operación de los servicios, aplicaciones y componentes que permiten al Instituto disponer de las capacidades de infraestructura de procesamiento, almacenamiento, respaldo, comunicaciones, seguridad, plataformas tecnológicas y software, que hoy en día se encuentran desplegadas en las siguientes ubicaciones:

- CDP - Centro de Datos Primario (Ambientes Productivos y no Productivos)
- ENP - Extensión de Nube Privada (ATOM)
- SDI - Servicios desplegados en Instalaciones designadas por el Instituto

Centro de Datos Primario

El Instituto habilitará los mecanismos idóneos para garantizar la continuidad operativa, soporte y gestión de la operación de la infraestructura actual del centro de datos primario (aplicaciones, servicios, infraestructura de procesamiento, almacenamiento y respaldo, infraestructura de seguridad y telecomunicaciones), en tanto se lleva a cabo la migración del Centro de Datos Actual a la infraestructura del Centro de Datos ofertado por **KIO Networks**, garantizando la operación de los aplicativos, servicios e infraestructura, de acuerdo a los niveles de servicio establecidos 99.982% de disponibilidad.

Extensión de Nube Privada (ATOM)

KIO Networks brindará continuidad del servicio, soporte y gestión de la operación 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.

Servicios desplegados en instalaciones designadas por el Instituto

KIO Networks brindará continuidad del servicio, soporte y gestión de la operación de infraestructura, por ejemplo, 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.

Ambientes no productivos en el Centro de Datos

KIO Networks brindará continuidad operativa, soporte y gestión de la operación de la infraestructura actual del centro de datos que contenga ambientes no productivos (aplicaciones no productivas, servicios, infraestructura de procesamiento, almacenamiento y respaldo, infraestructura de seguridad y telecomunicaciones), así como su migración del Centro de Datos Actual a la infraestructura del Centro de Datos ofertado por **KIO Networks**,

ANEXOS
DIVISIÓN DE CONTRATOS

garantizando la operación de los aplicativos, servicios e infraestructura, de acuerdo a los niveles de servicio establecidos 99.982% de disponibilidad.

Comunicaciones

KIO Networks brindará continuidad operativa, soporte y gestión de la operación de la solución de telecomunicaciones, incluyendo acciones para habilitación de infraestructura de conectividad en red con la funcionalidad de "Punto Neutro" durante el primer semestre del servicio, la cual deberá tener la capacidad de concentrar los enlaces de telecomunicaciones de las diferentes redes de telecomunicaciones del IMSS y proporcionadas por diversos prestadores de servicio, así como los enlaces de telecomunicaciones de los principales organismos públicos y privados con los que el Instituto interactúa. El servicio incluye la conectividad actual de 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.

KIO Networks brindará la continuidad a los servicios, aplicativos, servicios digitales y de información, así como su interconexión con los centros de datos propios del Instituto o del Gobierno Federal y entidades externas (tales como: SAT, RENAPO, Procesar, Banco de México, INFONAVIT, Bancos, Instituto Nacional Electoral, Afores, CONSAR, entre otros) que permitan el intercambio de información, conforme a los estándares de telecomunicaciones y seguridad definidos por el Instituto.

3 REQUERIMIENTOS TECNICOS

KIO Networks brindará continuidad operativa, soporte y gestión de la operación de la solución de infraestructura de procesamiento, almacenamiento, respaldos, telecomunicaciones y seguridad, así como a las aplicaciones, componentes y servicios digitales del Instituto en sus diversos esquemas desplegados, tales como: Centro de Datos Actual, Nodo de Extensión de Nube y Ubicaciones designadas por el Instituto, así como las que el Instituto designe durante la vigencia del Servicio.

Los servicios requeridos por el Instituto y que **KIO Networks** proveerá durante la vigencia del servicio son los siguientes:

- Servicio de Continuidad Operativa y Soporte
- Servicio de Continuidad y Soporte de Telecomunicaciones
- Servicio de Continuidad y Soporte de Seguridad

Para cada servicio antes mencionado, **KIO Networks** integrará como parte de la ejecución del servicio, los esquemas de Gestión de la Operación y Soporte, así como el Aprovisionamiento de infraestructura bajo demanda relativa a procesamiento, almacenamiento, respaldos, telecomunicaciones y seguridad.

La siguiente tabla muestra de manera enunciativa más no limitativa el esquema de organización de cada servicio:

Nombre del Servicio	Continuidad y Soporte bajo demanda	Aprovisionamiento de Infraestructura bajo demanda
Servicio de Continuidad Operativa y Soporte a la Operación	Servicios bajo demanda de continuidad operativa, gestión de la operación y soporte de la infraestructura de procesamiento, almacenamiento y respaldos, así como a las aplicaciones,	Aprovisionamiento de infraestructura de procesamiento, almacenamiento y respaldos, bajo demanda.

DS JCHV DS JAR

Nombre del Servicio	Continuidad y Soporte bajo demanda	Aprovisionamiento de Infraestructura bajo demanda
	componentes y servicios digitales del Instituto en cualquiera de sus capas (web, aplicativa, base de datos, balanceo etc.)	
Servicio de Continuidad y Soporte de Telecomunicaciones	Servicios bajo demanda de continuidad operativa, gestión de la operación y soporte referente a componentes e infraestructura de telecomunicaciones, así como la interconexión entre los diferentes ecosistemas Institucionales, así como con otras entidades públicas y privadas.	Aprovisionamiento de infraestructura de telecomunicaciones, bajo demanda.
Servicio de Continuidad y Soporte de Seguridad	Servicios bajo demanda de continuidad operativa, gestión de la operación y soporte referente a componentes e infraestructura de seguridad física y lógica.	Aprovisionamiento de infraestructura de seguridad, bajo demanda.

KIO Networks proveerá el soporte técnico en caso de falla en un esquema de 7 días 24 horas durante la vigencia del servicio.

A continuación, se describe el objetivo de cada servicio requerido por el Instituto y que **KIO Networks** brindará como parte de los servicios.

4 PLAZO DE LOS SERVICIOS

La vigencia del contrato y el plazo para la para la prestación del servicio será a partir del día siguiente de la fecha de adjudicación y hasta el 31 de diciembre de 2022

La definición de la programación, implementación y desarrollo de los servicios se establece en el correspondiente Anexo Técnico.

5 PERFIL DEL PROVEEDOR

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 entregará 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.

KIO Networks

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

KIO Networks cuenta con experiencia comprobable de al menos 5 años para brindar los servicios objeto del presente anexo técnico, apéndices, así como términos y condiciones, para lo cual se presentarán copia de contratos, pedidos o convenios formalizados con el sector público o privado cuyo objeto esté relacionado con los servicios de la presente licitación.

KIO Networks cuenta con especialidad comprobable de al menos 5 contratos formalizados cuyo objeto esté relacionado con la prestación de servicios similares al de la presente licitación.

KIO Networks cumple con las siguientes certificaciones de Centros de Datos así como, de Gestión del Servicio que se listan de manera enunciativa más no limitativa en la siguiente tabla:

Componente o Servicio	Descripción	Especificación	Tipo
Certificación de Centros de Datos	Certificación de Disponibilidad del Centro de Datos Ofertado	TIER III o ICREA IV equivalente o superior	Funcional
Gestión de Servicios de Tecnologías de la Información y Comunicaciones.	Certificación de gestión de procesos de Tecnologías de la Información y Comunicaciones.	ITIL V3 equivalente o superior	Funcional
Sistemas de Gestión del Servicio	Calidad en la Gestión de Servicios de TIC	ISO/IEC 20000-1 equivalente o superior	Funcional
Gestión de Seguridad de la Información	Implementación, Mantenimiento y Gestión de Sistemas de Gestión de Seguridad de la Información	ISO 27001 equivalente o superior	Funcional

Certificaciones enunciativas más no limitativas, o en su caso, similares en funcionalidad o tema en:

- **ISO/IEC 27001**
- **ISO/IEC 20000**
- **ITIL Expert Certificate**
- **ITIL Foundation Certificate in IT Service Management**
- **ITIL intermediate in Operational support and analysis**
- **ITIL intermediate in Service Offering AND Agreements**
- **ITIL intermediate un Release, control and validación**

El Administrador de proyectos deberá contar con las siguientes certificaciones:

- **Project Management Institute (PMI)**
- **ITIL Foundation Certificate in IT Service Management version 4**
- **Scrum Certified Master**

KIO Networks cuenta con el personal certificado en Metodologías de Administración de Proyectos para la dirección del proyecto.

KIO Networks cuenta con el personal certificado o con experiencia comprobable en productos, software y componentes descritos en el presente anexo técnico por lo que se adjunta a la propuesta las siguientes certificaciones:

- **CCNA - Cisco Certified Network Associate**
- **CCNA - Cisco Certified Network Associate Routing and Switching**
- **CCNP - Cisco Certified Network Professional**
- **Cisco Certified Specialist - Data Center Core**
- **CISM - Certified Information Security Manager**
- **CISSP Certified Information Systems Security Professional**
- **MCITP Enterprise Administrator on Windows Server 2008**
- **MCTS Microsoft Exchange Server 2007 Configuration**
- **Scrum Master Certified Credential**
- **Exchange Server 2007 Configuration**
- **Windows Server 2008 Active Directory, Configuring**
- **Windows Server 2008 Applications Infrastructure, Configuring**
- **Windows Server 2008 Network Infrastructure, Configuring**
- **Windows Server 2008, Enterprise Administrator**
- **Microsoft SQL Server 2008, Implementation and Maintenance**
- **Oracle Certified Associate - Oracle WebLogic Server 11g System Administrator**
- **Oracle Database 11g: Administrator Certified Associate**
- **Oracle Database 11g: Administrator Certified Professional**
- **Oracle Database 12c Certified Implementation Specialist**
- **Oracle WebLogic Server 12c Administrator**
- **Oracle VM 3.0 for x86 Certified Implementation Specialist**
- **VMware Certified Professional Data Center Virtualization 2019 o superior**
- **Querying Microsoft SQL Server 2012/2014 o superior**
- **Administering Microsoft SQL Server 2012/2014 Databases**
- **Implementing a Data Warehouse with Microsoft SQL Server 2012/2014**
- **Microsoft Certified Solutions Associate SQL Server 2012/2014**
- **Red Hat Certified System Administrator Enterprise Linux 6 o superior**

El **INSTITUTO** podrá solicitar en cualquier momento del proceso de contratación y durante la vigencia del contrato, los originales de las certificaciones presentadas por **KIO Networks** para su cotejo, mismas que serán devueltas una vez concluida la revisión.

KIO Networks presentará al Instituto, a través de la Coordinación de Servicios de Infraestructura Tecnológica Institucional cita en Toledo 21 6to piso, 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 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, el plan de trabajo, 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 acorde a lo descrito en el anexo técnico y con los que el Instituto estará colaborando, su cargo y puesto, así como los datos y la vía de comunicación para contactarlo.

KIO Networks

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

6 CUMPLIMIENTO DE OBLIGACIONES CONTRACTUALES

Para la documentación de Cumplimiento de Obligaciones contractuales, **KIO Networks** 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 de **KIO Networks**, a fin de contar con un listado de todos los verbos de acción, 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 **KIO Networks**, 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 **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 **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** expondrá 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 **KIO Networks**, éste deberá habilitar 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) 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 la Coordinación de Servicios 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 **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 el licitante no cuente 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.

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; es 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 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

ANEXOS
DIVISIÓN DE CONTRATOS

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.

8 ADMINISTRADORES DEL CONTRATO

El administrador del Contrato será el Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional, mismo que conforme a sus atribuciones será el encargado de verificar que los servicios que administran se entreguen en los tiempos y las formas establecidos en el Anexo Técnico.

9 DERECHOS DE AUTOR

KIO Networks presentará escrito, a más tardar a los 05 (cinco) días naturales de la adjudicación del contrato, 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.

KIO Networks

DS JCHV DS JAR

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 **KIO Networks** y sea propiedad exclusiva del Instituto.

Por lo anterior, **KIO Networks** 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, así como al artículo 8 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

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, **KIO Networks** 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 **KIO Networks** designe para la prestación de los servicios materia del presente proceso de contratación, es considerada de carácter confidencial, por lo que **KIO Networks** garantizará que por ningún motivo se viole ninguno de los siguientes acuerdos:

    a. La información del IMSS y a la cual tenga acceso el personal de **KIO Networks**, no será copiada o respaldada en ninguno de los equipos del personal de **KIO Networks** 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 de **KIO Networks**, 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 **KIO Networks**.

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

KIO Networks

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

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.

11 CONFORMACION DE LA PROPUESTA

KIO Networks en la presente contratación entregará, de manera obligatoria, la Propuesta Técnica para realizar la respectiva evaluación.

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

KIO Networks integrará 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 con lo explicado en este documento.

KIO Networks presentará 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 contendrá 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 de **KIO Networks**, 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. **KIO Networks** se asegurará 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

KIO Networks 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 **KIO Networks** 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 **KIO Networks** traduzca sólo el párrafo(s) que es de interés para el punto que se está documentando o citando, siempre y cuando **KIO Networks** haga entrega del resto de la documentación en su formato e idioma original o traducción simple al español. 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

KIO Networks integrará 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

ANEXOS
DIVISIÓN DE CONTRATOS

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 deben emplear el mismo orden y secuencia de temas que comprenden dichos documentos, 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.
02	Descripción a alto nivel de la arquitectura global que **KIO Networks** 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 **KIO Networks** 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

No	Entregable
	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 GARANTIAS

Garantía de cumplimiento de contrato

KIO Networks para garantizar el cumplimiento de todas y cada una de las obligaciones estipuladas en el contrato adjudicado, deberá presentar fianza expedida por afianzadora debidamente constituida en términos de la Ley de Instituciones de Seguros y Fianzas, por un importe equivalente al 10% (diez por ciento) del monto máximo del contrato, sin considerar el impuesto al valor agregado, a favor del Instituto.

La garantía deberá presentarse dentro del término 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 4.24.4 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.

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

Garantía de Servicios.

Respecto de Garantías de Servicio, **KIO Networks** presentará 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.

13 NIVELES DE SERVICIO

El Servicio de Continuidad de la Nube IMSS 2022 se sujetará a los niveles de servicio establecidos en el apéndice respectivo del Anexo Técnico correspondiente.

KIO Networks®

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

14 PENAS CONVENCIONALES Y DEDUCTIVAS

- Las penas convencionales y deductivas se calcularán conforme a lo establecido en el Apéndice 6 "Métricas de Niveles de Servicio".
- 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, **KIO Networks** 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 **KIO Networks** 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 de **KIO Networks** y del personal que ejecuta los procesos de Negocio por parte del Instituto.
- Delimitar las funciones entre **KIO Networks** 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.

KIO Networks, 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.

16 UBICACIONES PARA LA PRESTACION DEL SERVICIO

KIO Networks tiene la obligación de prestar sus servicios en las 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 FINALIZACION DEL CONTRATO

KIO Networks toma 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 este 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, **KIO Networks** 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.

KIO Networks 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

Se efectuarán pagos a " **KIO Networks** " una vez proporcionado los servicios, de conformidad con lo dispuesto en los artículos 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 93 de su Reglamento, así como por lo establecido en los Términos y Condiciones que se agreguen al contrato.

El pago del servicio se realizará en "EL INSTITUTO", cuyos domicilios se relacionan en el Anexo correspondiente del contrato, una vez que el servicio haya sido proporcionado conforme al anexo técnico:

El pago se realizará en pesos mexicanos, en los plazos normados por la Dirección de Finanzas en el "Procedimiento para la recepción, glosa v 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 " **KIO Networks** " presente en las áreas de trámite de erogaciones la representación impresa del Comprobante Fiscal Digital por Internet (CFDI), siempre y cuando se cuente con la suficiencia presupuestal, así como con la documentación comprobatoria que acredite la prestación de los servicios, y se indique en dicha documentación los servicios proporcionados, número de proveedor, número de contrato, número de fianza y denominación social de la afianzadora, en su caso.

KIO Networks

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

" **KIO Networks** " expedirá 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 IMS471231I45, domicilio en Avenida Paseo de la Reforma número 476, Colonia Juárez, Código Postal 06600, Demarcación Territorial Cuauhtémoc, en la Ciudad de México.

" **KIO Networks** ", para cada uno de los pagos que efectivamente reciba, de acuerdo con esta cláusula, expedirá 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 " **KIO Networks** " cargará 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, " **KIO Networks** " proporcionará con oportunidad su número de cuenta, CLABE, banco y sucursal, a menos que " **KIO Networks** " 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 " **KIO Networks** " 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 de los servicios, sí no se ha determinado, calculado y notificado a " **KIO Networks** " las penas convencionales o deducciones pactadas en el presente contrato, así como su registro y validación en el Sistema PREI Millenium.

" **KIO Networks** " 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.

" **KIO Networks** " entregará 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.

" **KIO Networks** ", durante la vigencia del 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". (En caso de aplicar)

KIO Networks

DS JCHV DS JAR

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 (en caso de aplicar).

Para que " **KIO Networks** " pueda celebrar un contrato de cesión de derechos de cobro, deberá notificarlo por escrito a "ELINSTITUTO" 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 " **KIO Networks** " 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 " **KIO Networks** " 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 " **KIO Networks** " las deficiencias o errores que deberá corregir. El periodo que transcurra a partir de la entrega del citado escrito y hasta que " **KIO Networks** " 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 SS Bis, segundo párrafo de la Ley de Adquisiciones. Arrendamientos y Servicios del Sector Público, previa solicitud por escrito a " **KIO Networks** ", 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, o ante la Jefatura de Servicios de Finanzas o de la UMAE correspondiente. (Eliminar lo marcado cuando el pago se efectúe a Nivel Central o ante los Órganos de Operación Administrativa Desconcentrada).

KIO Networks®

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

El pago de los servicios quedará condicionado proporcionalmente al pago que " **KIO Networks** " 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.

19 MECANISMOS DE CONTROL PARA LA ADMINISTRACION

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 **KIO Networks**, incurra en incumplimiento de cualquiera de las obligaciones a su cargo, de conformidad con el procedimiento siguiente.

Si el Instituto considera que **KIO Networks** ha incurrido en alguna de las causales de rescisión que se consignan más adelante, lo hará saber a **KIO Networks**, 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 a **KIO Networks**. La determinación de dar o no por rescindido el contrato deberá ser debidamente fundada, motivada y comunicada a **KIO Networks** dentro dicho plazo.

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 **KIO Networks**, 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, **KIO Networks**, 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.

KIO Networks

DS JCHV DS JAR

De no darse por rescindido el contrato, el Instituto, establecerá de conformidad con **KIO Networks**, un nuevo plazo para el cumplimiento de aquellas obligaciones que se hubiesen dejado de cumplir, a efecto de que **KIO Networks**, 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 **KIO Networks** 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 de **KIO Networks**
4. Cuando de manera reiterativa y constante, **KIO Networks** 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 a **KIO Networks**, 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.
6. Si la aplicación de las penas convencionales rebasa el monto de la garantía de cumplimiento del contrato.

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).

20 CRITERIO DE EVALUACION

La evaluación de las proposiciones se realizará utilizando el criterio de puntos, considerando exclusivamente los requisitos y condiciones establecidos en el anexo técnico, términos y condiciones, así como en el formato de propuesta económica, a efecto de que se garantice satisfactoriamente el cumplimiento de las obligaciones respectivas.

En esta modalidad, la adjudicación se hará a **KIO Networks** una vez obtenido el mayor puntaje en cuanto a su propuesta técnica y económica, en su caso, para lo no previsto será aplicable lo establecido en los *"LINEAMIENTOS PARA LA*

ANEXOS
DIVISIÓN DE CONTRATOS

APLICACIÓN DEL CRITERIO DE EVALUACIÓN DE PROPOSICIONES A TRAVÉS DEL MECANISMO DE PUNTOS O PORCENTAJES EN LOS PROCEDIMIENTOS DE CONTRATACIÓN" publicados en el Diario Oficial de la Federación.

La propuesta económica más baja tendrá el puntaje más alto siendo éste de 40 puntos, el valor de las propuestas económicas mayores a la más baja se obtendrá de la siguiente operación:

PPE = MPemb x 40 / MPi.

Dónde:
PPE *= Puntuación o unidades porcentuales que corresponde a la Propuesta Económica*
MPemb *= Monto de la Propuesta Económica más baja, y*
MPi *= Monto de la i-ésima Propuesta Económica.*

Se aceptarán las ofertas que cumplan con los requerimientos establecidos y cubran las características técnicas establecidas en el anexo técnico.

La evaluación por el mecanismo de puntos y porcentajes consta de 100 puntos, de los cuales 40 puntos corresponden a la propuesta económica considerando el monto total de la propuesta conforme al formato de propuesta económica.

Los 60 puntos restantes corresponden a la evaluación técnica, que consiste en la suma de la puntuación de los siguientes rubros, con sus respectivos apartados:

NÚMERO DE RUBRO	RUBRO	PUNTUACIÓN PARA OTORGAR
I	CAPACIDAD DEL LICITANTE	
II	EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE	
III	PROPUESTA DE TRABAJO	
IV	CUMPLIMIENTO DE CONTRATOS	
TOTAL		

Para que la propuesta sea considerada solvente y, por tanto, no ser desechada, deberá obtener una puntuación de cuando menos 45 de los 60 máximos a obtener en la evaluación.

La omisión total o parcial en la presentación de alguno de los rubros a evaluar NO será motivo de des echamiento. No obstante, lo anterior, en tal caso el Instituto se abstendrá de asignar puntos en el rubro correspondiente.

Consiste en el número de recursos humanos que técnicamente estén aptos para prestar el servicio, así como los recursos económicos y de equipamiento que requiere **KIO Networks** para prestar los servicios en el tiempo, condiciones y niveles de calidad requeridos por **"EL INSTITUTO"**, así como otorgar cualquier otro aspecto indispensable para que **"KIO Networks** pueda cumplir con las obligaciones previstas.

#	CARACTERÍSTICAS Servicio de continuidad de la Nube IMSS 2022	VERIFICACION REFERENCIA	PUNTOS MÁXIMOS	OBSERVACIONES
1	**A) Capacidad del Licitante**			
	Consiste en los recursos con que cuente el licitante para la prestación de los servicios materia de la presente convocatoria, tales como: recursos humanos técnicamente aptos para prestar el servicio, así como los recursos económicos y de equipamiento que requiere el licitante para prestar los servicios en el tiempo, condiciones y			

DS DS

#	CARACTERÍSTICAS **Servicio de continuidad de la Nube IMSS 2022**	VERIFICACION REFERENCIA	PUNTOS MÁXIMOS	OBSERVACIONES
	niveles de calidad requeridos por la convocante; así como cualquier otro aspecto indispensable para que el licitante pueda cumplir con las obligaciones previstas en el contrato.			
	a) Capacidad de los recursos humanos.			
	Experiencia			
	Presentar manifestación por cada uno de los perfiles, firmada por el representante legal de la empresa licitante, en la que manifieste que los recursos cuentan con algunas de las certificaciones siguientes: ISO/IEC 27001 ISO/IEC 20000 ITIL Expert Certificate ITIL Foundation Certificate in IT Service Management ITIL intermediate in Operational support and analysis ITIL intermediate in Service Offering AND Agreements ITIL intermediate un Release, control and validación Project Management Institute (PMI) ITIL V4 SCRUM Certified Master Asimismo deberá manifestarlo por cada uno de los siguientes perfiles:		XX	
	· Que cuenta con al menos 1 (una) persona que se encuentren dentro de su plantilla la cual deberá tener al menos 3 años de experiencia en proyectos de tecnologías de la información, como Administrador de proyectos y con certificación vigente en Project Manager Professional (PMP) emitida por el Project Management Institute (PMI).ITIL Foundation Certificate in IT Service Management version 4 y Certified ScrumMaster			
	· Que cuenta con al menos 1 (una) persona que se encuentre dentro de su plantilla la cual deberá tener al menos 3 Años de experiencia en proyectos de tecnologías de la información realizando actividades como Gestor del Proceso de Gestión de Requerimientos de acuerdo a las actividades descritas en el Anexo Técnico			
	· Que cuenta con al menos 1 (una) persona que se encuentre dentro de su plantilla la cual deberá tener al menos 3 Años de experiencia en proyectos de tecnologías de la información realizando actividades como Gestor del Proceso de Gestión de Incidentes, de acuerdo a las actividades descritas en el Anexo Técnico			

KIO Networks

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

#	CARACTERÍSTICAS	VERIFICACION	PUNTOS	OBSERVACIONES
	Servicio de continuidad de la Nube IMSS 2022	**REFERENCIA**	**MÁXIMOS**	
	· Que cuenta con al menos 1 (una) persona que se encuentre dentro de su plantilla la cual deberá tener al menos 3 Años de experiencia en proyectos de tecnologías de la información, realizando actividades como Gestor del Proceso de Gestión de Problemas, de acuerdo a las actividades descritas en el Anexo Técnico			
	· Que cuenta con al menos 1 (una) persona que se encuentre dentro de su plantilla la cual deberá tener al menos 3 Años de experiencia en proyectos de tecnologías de la información realizando actividades como Gestor de cambios, de acuerdo a las actividades descritas en el Anexo Técnico			
	· Que cuenta con al menos 1 (una) persona que se encuentre dentro de su plantilla la cual deberá tener al menos 3 años de experiencia en proyectos de tecnologías de la información realizando actividades como Gestor del proceso de gestión de liberaciones, de acuerdo a las actividades descritas en el Anexo Técnico			
	· Que cuenta con al menos menos 1 (una) persona que se encuentre dentro de su plantilla la cual deberá tener al menos 3 años de experiencia en proyectos de tecnologías de la información realizando actividades como Coordinador de licenciamiento y versionamiento, de acuerdo a las actividades descritas en el Anexo Técnico			
	· Que cuenta con al menos menos 1 (una) persona que se encuentre dentro de su plantilla la cual deberá tener al menos 3 años de experiencia en proyectos de tecnologías de la información realizando actividades como Coordinador de configuraciones, de acuerdo a las actividades descritas en el Anexo Técnico			
	· Que cuenta con al menos 1 (una) persona que se encuentre dentro de su plantilla la cual deberá tener al menos 3 años de experiencia en proyectos de tecnologías de la información realizando actividades como Coordinador de Proyecto de Soporte Extendido, de acuerdo a las actividades descritas en el Anexo Técnico			
	Los licitantes deberán presentar el currículum vitae del personal designado, cumpliendo con los siguientes requisitos:			
	- Nombre completo del recurso a asignar			
	- Experiencia profesional: Donde se señalen el nombre de la empresa o entidad donde presto sus servicios, los cargos que haya desempeñado, periodos de prestación de servicios, nombre de los empleadores, nombre de los cargos que ha ejercido y el tipo de funciones bajo su responsabilidad			

KIO Networks

DS JCHV DS JAR

#	CARACTERÍSTICAS **Servicio de continuidad de la Nube IMSS 2022**	VERIFICACION REFERENCIA	PUNTOS MÁXIMOS	OBSERVACIONES
	- Estudios: bajo este rubro se anotarán todos los estudios relacionados con el objeto del servicio, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica.			
	Así como copia simple de los contratos de trabajo u hojas de afiliación al Seguro Social.			
	Nota: Se dará una puntuación de XX **puntos** por cada uno de los perfiles que cumplan con los requisitos solicitados y entreguen la documentación completa otorgando como máximo XX **puntos**, en caso de no presentar la documentación correspondiente se considerará **como 0.00 la puntuación.**			
	Competencia o habilidad en el trabajo de acuerdo con sus conocimientos académicos o profesionales			
	El licitante deberá comprobar que el personal solicitado en el rubro anterior cuenta con estudios en Ingeniería o licenciatura en computación o carreras afines a tecnologías de información y comunicaciones, por lo que deberá presentar:			
	· Título y/o Cédula profesional para cada perfil propuesto			
	· Certificaciones (vigentes) mínimas requeridas por perfil propuesto			
	Las certificaciones por cada perfil que se presenten en un idioma diferente al español deberán adjuntar la traducción simple al español.			
	Nota: Por cada persona de las designadas en los puntos anteriores que acredite que cuenta con ambos documentos que cumplan con los requisitos establecidos, se le otorgarán XX **puntos** y se le otorgara **un máximo de XX puntos**; en caso de no entregar la totalidad de la documentación que cumpla con los requisitos establecidos no se le otorgará puntuación.			
	Dominio de Herramientas			
	El licitante deberá comprobar que cuenta con las certificaciones vigentes relacionadas con la prestación del servicio que se listan a continuación:			
	· TIER III ó ICREA IV equivalente o superior			
	· ISO/IEC 27001			
	· ISO/IEC 9001			
	· ISO/IEC 20000			

KIO Networks

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

#	CARACTERÍSTICAS	VERIFICACION	PUNTOS	OBSERVACIONES
	Servicio de continuidad de la Nube IMSS 2022	**REFERENCIA**	**MÁXIMOS**	
	Las certificaciones presentadas por parte de la empresa podrán ser presentadas en su idioma original y su traducción simple al español. Las certificaciones deberán estás vigentes al momento de la presentación y apertura de propuestas.			
	Se otorgarán XX **puntos** por cada certificación presentada, **siendo el máximo de puntos a otorgar XX puntos.** Los licitantes que no presenten estas certificaciones será desechada su propuesta técnica			
	b) Capacidad de Recursos Económicos y Equipamiento			
	b1) Recursos económicos			
	El Licitante deberá entregar copia simple de la última declaración fiscal anual del impuesto sobre la renta (ISR ejercicio 2020) presentada ante el Servicio de Administración Tributaria (SAT), y de las declaraciones provisionales acompañadas de sus respectivos acuses, correspondientes al ejercicio fiscal 2021 y hasta el mes que corresponda previo a la fecha del acto de presentación y apertura de proposiciones.			
	Los documentos anteriores deberán acreditar que sus ingresos durante 2020 y lo relativo a 2021 equivalen al menos a un porcentaje del 20% del monto total de su oferta económica.			
	Al licitante que entregue toda la documentación requerida, (No se aceptaran cartas bajo protesta de decir verdad), donde se demuestre que cumplen con lo solicitado en el Anexo Técnico y su Apéndice, se le darán una **calificación máxima de XX puntos**. Quien no presente la información completa solicitada donde se pueda comprobar su cumplimiento, tendrá 0.00 puntos.			
	b2) Equipamiento			
	El licitante, deberá adjuntar documento con la ficha técnica de los componentes de la solución propuesta para la prestación del servicio y el mecanismo para el reemplazo del equipo propuesto en los casos que se requiera. Conforme a las especificaciones descritas en el Anexo Técnico.			
	Al licitante que entregue toda la documentación requerida, (No se aceptaran cartas bajo protesta de decir verdad), donde se demuestre que cumplen con lo solicitado en el Anexo Técnico y su Apéndice, se le darán una **calificación máxima de XX puntos**. Quien no presente la información completa solicitada donde se pueda comprobar su cumplimiento, **tendrá 0.00 puntos.**			
	Participación de discapacitados o empresas que cuenten con trabajadores con discapacidad			

KIO Networks

DS JCHV DS JAR

#	CARACTERÍSTICAS **Servicio de continuidad de la Nube IMSS 2022**	VERIFICACION REFERENCIA	PUNTOS MÁXIMOS	OBSERVACIONES
	Se otorgará puntaje al licitante que cuente cuando menos con el 5% de la totalidad de su plantilla de empleados con discapacidad, cuya antigüedad no sea inferior a seis meses, misma que se comprobará con la siguiente documentación:			
	Aviso de alta al régimen obligatorio del Instituto Mexicano del Seguro Social, constancias o certificados de reconocimiento de discapacidad, expedidos por alguna institución del sector salud federal y cédula de determinación y comprobación de pago al IMSS correspondiente al mes de enero de 2018.			
	Se asignará la mayor puntuación que **corresponde a XX**, al licitante que acredite tener el mayor número de trabajadores discapacitados en los términos señalados en el presente rubro. A partir del o los licitantes que hubieren obtenido mayor puntuación, se distribuirá, de manera proporcional la puntuación o unidades porcentuales a los demás licitantes, aplicando para ello una regla de tres.			
	Para el caso que no le sea aplicable este criterio, bastará con que el licitante presente un formato refiriéndose a este rubro con la leyenda "No Aplica"			
	Participación de MIPYME			
	Se otorgará puntaje a la MIPYME participante que tenga alguna innovación tecnológica relacionada con alguno de los bienes o servicios que sean proporcionados con motivo del cumplimiento de las obligaciones contractuales para lo cual se presentará el siguiente documento:			
	Constancia emitida por el instituto mexicano de la propiedad industrial, la cual no podrá tener una vigencia mayor a cinco años.			
	Si el licitante presenta constancia emitida por el Instituto Mexicano de la Propiedad Industrial, **se le otorgarán XX puntos**. Si el licitante no presenta constancia emitida por el Instituto Mexicano de la Propiedad Industrial, se le otorgarán 0.00 puntos.			
	Para el caso que no le sea aplicable este criterio, bastará con que el licitante presente un formato refiriéndose a este rubro con la leyenda "No Aplica"			
	Certificación de políticas y prácticas de igualdad de género.			
	Se otorgarán puntos a las empresas que hayan aplicado políticas y prácticas de igualdad de género, conforme a la certificación correspondiente emitida por las autoridades y organismos facultados para tal efecto.			

KIO Networks

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

#	CARACTERÍSTICAS	VERIFICACION	PUNTOS	OBSERVACIONES
	Servicio de continuidad de la Nube IMSS 2022	**REFERENCIA**	**MÁXIMOS**	
	En su caso, el licitante deberá presentar copia del certificado emitido por las autoridades de haber aplicado políticas y prácticas de igualdad de género. Al licitante que presente las políticas aplicadas **se le dará XX puntos**. De no encontrarse la Licitante en el presente caso no será necesario entregar carta o documento alguno.			
	Para el caso que no le sea aplicable este criterio, bastará con que el licitante presente un formato refiriéndose a este rubro con la leyenda "No Aplica"			
	Total Puntos por este Rubro			
2	**B) Experiencia y especialidad del Licitante**			
	a) Experiencia			
	El licitante deberá acreditar que cuenta con al menos 1 año y máximo 8 años de experiencia. para lo cual deberá acreditar el mayor número de contratos, pedidos, facturas u órdenes de servicio con las características y condiciones afines o similares a los requeridos en el procedimiento de contratación, con un monto total agregado de cuando menos el 50% del monto total de su oferta, para lo cual deberá presentar mínimo 1y máximo 10 contratos, pedidos, facturas u órdenes de servicio con institución pública o empresa privada, legibles, firmados, concluidos antes del acto de presentación y apertura de proposiciones, a efecto de que sean susceptibles de computarse el número de contratos, pedidos, facturas u órdenes de servicio similares a los requeridos en este procedimiento, con los que acredite su especialidad en la prestación de servicios adjuntando una cédula en formato libre donde relacione los mismos, el sujeto o institución contratante; su vigencia y número de documento contractual.			
	Tratándose contratos, pedidos, facturas u órdenes de servicio celebrados con particulares, se deberá exhibir además la última factura de pago validada y vigente.			
	En el caso de las facturas, además de cumplir con todos los requisitos fiscales, deberán contener los datos que identifiquen el servicio, como son la fecha, el monto, el cliente, debidamente validada la CFDI ante el portal del SAT en la siguiente liga https://verificacdfdi.facturaelectronica.sat.gob y vigentes en el portal del SAT			
	En caso de exhibir más de 10 contratos, pedidos, facturas u órdenes de servicio sólo se valuarán los 10 primeros considerando el número de folio y sólo se considerarán los contratos, pedidos, facturas u órdenes de servicio que hayan sido celebrados en los últimos 10 años.			

KIO Networks

DS JCHV DS JAR

#	CARACTERÍSTICAS **Servicio de continuidad de la Nube IMSS 2022**	VERIFICACION REFERENCIA	PUNTOS MÁXIMOS	OBSERVACIONES
	El licitante podrá exhibir los mismos contratos que hubiere exhibido para acreditar la especialidad o cumplimiento de contratos siempre y cuando estos estén concluidos a la fecha de presentación y apertura de proposiciones. En caso de no exhibir contratos, pedidos y facturas no será acreedor a puntos. En caso de que el licitante exhiba los documentos y que sus vigencias se empalmen, sólo se considerará el tiempo efectivamente transcurrido.			
	1) Proemio, declaraciones y objeto. si los servicios no se describen claramente en el objeto, el licitante deberá incluir adicionalmente la parte del contrato que los contenga.			
	2) Indicar el nombre y/o razón social del cliente.			
	3) Información adicional que el licitante considere útil para verificar y validar las referencias proporcionadas.			
	4) El licitante deberá indicar con claridad cómo y en qué sección de los contratos presentados se cumple cada uno de los puntos solicitados en este apartado.			
	A los licitantes participantes que acrediten su experiencia en la prestación de servicios similares al de la presente licitación se les asignarán puntos conforme a los siguientes **Rangos: 8 años de experiencia (X puntos); 7 años de experiencia (X puntos); 6 años de experiencia (X puntos); 5 años de experiencia (X puntos); 4años de experiencia (X puntos); 3 años de experiencia (X puntos); 2 años de experiencia (x puntos); 1 año de experiencia (X puntos); 0 años de experiencia (0 puntos).**			
	Al licitante que no cumpla con al menos 5 años de experiencia con al menos 5 contratos **no se le otorgará puntuación.**			
	Los contratos que presente para este rubro podrán ser los mismos que presente para acreditar la Especialidad del Licitante. Si el Licitante comprueba más de 8 años de experiencia, solo se otorgarán puntos por el máximo de años indicado para este rubro.			
	b) Especialidad del Licitante			
	Deberá de entregar copia simple de contratos o pedidos para lo cual deberá presentar mínimo 1 máximo 10 cuyo objeto esté relacionado con la prestación de servicios similares al de la presente licitación.			

KIO Networks®

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

#	CARACTERÍSTICAS	VERIFICACION	PUNTOS	OBSERVACIONES
	Servicio de continuidad de la Nube IMSS 2022	**REFERENCIA**	**MÁXIMOS**	
	El licitante acreditará el mayor tiempo prestando servicios similares a los requeridos en el procedimiento de contratación, mediante la presentación de contratos.			
	Para acreditar la especialidad, el licitante presentará contratos, pedidos, facturas u órdenes de servicio celebrados con institución pública o empresa privada completos, legibles, firmados cuya formalización hubiera sido dentro del rango de mínimo 1 año y máximo 10 años anterior a la fecha de la presentación y apertura de proposiciones, a efecto de que sean susceptibles de computarse los años en los que hayan prestado servicios similares a los requeridos en este procedimiento, adjuntado una cédula en formato libre donde relacione los mismos, el sujeto o institución contratante; su vigencia y número del documento contractual			
	Tratándose de contratos celebrados con particulares, se deberá exhibir además la última factura de pago.			
	En el caso de las facturas, además de cumplir con todos los requisitos fiscales, deberán contener los datos que identifiquen el servicio, como son la fecha, el monto, el cliente, debidamente validada la CFDI ante el portal del SAT en la siguiente liga: https://verificacfdi.facturalectronica.sat.gob. y vigentes en el portal del SAT a entre otros.			
	En caso de exhibir más de 10 (diez) contratos, pedidos, facturas u órdenes de servicio, solo se evaluarán los 10(diez) primeros considerando el número de folio.			
	En caso de que el licitante no presente completa la documentación solicitada, no será acreedor a puntos.			
	Los contratos, pedidos, facturas u órdenes de servicio podrán estar vigentes o concluidos a la fecha de la presentación y apertura de proposiciones, también se aceptarán contratos o pedidos plurianuales de los cuales sólo se computará el tiempo efectivamente prestado a la fecha de presentación y apertura de proposiciones.			
	El licitante podrá exhibir los mismos contratos, pedidos, facturas u órdenes de servicio que hubiere exhibido para acreditar la experiencia o cumplimiento de contratos, en caso de ser diferentes, éstos deberán ser bajo las mismas condiciones a los solicitados en el rubro de experiencia.			
	En caso de no exhibir contratos no será acreedor a puntos.			
	Al licitante que presente 10 contratos o pedidos de servicios similares al de la presente licitación se le **otorgarán X puntos**; al licitante que presente 8 contratos o pedidos de servicios similares al de la presente licitación **se le otorgarán X puntos,** al licitante que presente 6 contratos o			

KIO Networks

DS JCHV DS JAR

#	CARACTERÍSTICAS Servicio de continuidad de la Nube IMSS 2022	VERIFICACION REFERENCIA	PUNTOS MÁXIMOS	OBSERVACIONES
	pedidos de servicios similares al de la presente licitación **se le otorgarán X puntos,** al licitante que presente 4 contratos o pedidos de servicios similares al de la presente licitación **se le otorgarán X puntos,** al licitante que presente 2 contratos o pedidos de servicios similares al de la presente licitación **se le otorgarán X puntos.**			
	Total de Puntos por este rubro:			
3	**C) Metodología, Plan de trabajo y Organigrama**			
	C1) Metodología			
	El licitante se obliga a proporcionar al Instituto una **metodología** donde se describa la estrategia de implementación de la solución propuesta. Dicha metodología apegarse a lo establecido por el Project Management Institute (PMI) (inicio, planeación, ejecución, control y cierre)			
	Al licitante que entregue la metodología se le **otorgarán un máximo de X puntos.** Quien no presente la información completa solicitada **tendrá 0.00 puntos.**			
	C2) Plan de Trabajo			
	El licitante se obliga a proporcionar al Instituto un **plan de trabajo** donde se describa los recursos humanos y materiales de que dispone para prestar el servicio, cuándo y cómo llevará a cabo las actividades o tareas que implica el mismo.			
	El licitante deberá tener presente que el plan de trabajo solicitado deberá considerar la vigencia del servicio hasta su conclusión y establecer tiempos de respuesta ante cualquier incidente.			
	Al licitante que entregue el plan de trabajo con el menor tiempo de implementación se le **otorgarán un máximo de X puntos** bajo los siguientes criterios: De 0 a 30 días naturales se otorgarán X **puntos** De 31 a 60 días naturales se otorgarán **X puntos** De 61 a 90 días naturales se otorgarán X **puntos** Mas de 90 días naturales se otorgarán X **puntos** Quien no presente la información completa solicitada **tendrá 0.00 puntos.**			
	C3) Organigrama			

KIO Networks

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

#	CARACTERÍSTICAS Servicio de continuidad de la Nube IMSS 2022	VERIFICACION REFERENCIA	PUNTOS MÁXIMOS	OBSERVACIONES
	El licitante deberá proporcionar al Instituto una **matriz organizacional**, así como la matriz de escalación, indicando nombres y cargos de los responsables, teléfonos, e-mail y celulares. Quien presente dicha matriz se le **otorgará X puntos**. Quien no presente dicha matriz **tendrá 0.00 puntos.**			
	Total de Puntos por este rubro:			
4	**D) Cumplimiento de contratos**			
	Deberá de entregar copia simple de cartas de cumplimiento a satisfacción, liberación de fianza o documento que compruebe el total cumplimiento del mínimo 1 o máximo 10 contratos o pedidos con los cuales se compruebe que se proporcionaron servicios similares ya sea con Instituciones Privadas o Gubernamentales.			
	Al licitante que demuestre el cumplimiento satisfactorio de 10 contratos se le **otorgarán XX puntos**; al licitante que demuestre el cumplimiento satisfactorio de 8 contratos se le **otorgarán X puntos,** el cumplimiento satisfactorio de 3contratos se le **otorgarán X puntos.**			
	Al licitante que no acredite el cumplimiento satisfactorio de al menos 3 contratos no se le otorgarán puntos.			
	Las cartas de cumplimiento o documento que compruebe el total cumplimiento de los contratos.			
	Las cartas de cumplimiento, liberación de fianzas o documento que acredite el total cumplimiento de sus obligaciones, podrán ser de los mismos contratos presentados para Experiencia y Especialidad. El licitante podrá exhibir los mismos contratos, pedidos, facturas u órdenes de servicio que hubiere exhibido para acreditar la experiencia o especialidad, en caso de ser diferentes, éstos deberán ser bajo las mismas condiciones a los solicitados en el rubro de experiencia.			
	Total de Puntos por este rubro:			
	TOTAL DE PUNTOS OBTENIDOS			

21 LICENCIAS, PERMISOS, REGISTROS, CETIFICADOS O AUTORIZACIONES QUE DEBE CUMPLIR O APLCIARSE AL BIEN O SERVICIO A CONTRATAR

No aplica.

DS JCHV DS JAR

22 FOLETOS, CATALOGOS, FOTOGRAFIAS, MANUALES ENTRE OTROS, EN CASO DE QUE SE REQUIERAN PARA COMPROBAR LAS ESPECIFICACIONES TECNICAS REQUERIDAS

No aplica.

23 VISITAS A LAS INSTALACIONES INSTITUCIONALES, DONDE SE SUMINISTRARAN O COLOCARAN LOS BIENES O DONDE SE PRESTARAN LOS SERVICIOS, EN SU CASO

En caso de requerirse, el licitante podrá solicitar al instituto la visita a las instalaciones institucionales, donde se suministrarán o colocarán los bienes o donde se prestarán los servicios con al menos 5 días de anticipación a su visita

24 EN SU CASO, MECANISMOS REQUERIDOS AL PROVEEDOR PARA RESPONDER POR DEFECTOS O VICIOS OCULTOS DE LOS BIENES O DE LA CALIDAD DE LOS SERVICIOS

No aplica.

25 RESPONSABILIDAD

KIO Networks 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.

26 RESPONSABILIDAD LABORAL

Queda expresamente estipulado que el personal para la prestación del servicio o que utilice **KIO Networks** 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 a **KIO Networks** 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 a **KIO Networks** a responder de cualquier acción legal y/o reclamación que se pudiera presentar en contra del Instituto.

Independientemente de lo anterior, **KIO Networks** cumplirá 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).

KIO Networks

DS JCHV DS JAR

ANEXOS
DIVISIÓN DE CONTRATOS

27 FIRMAS DE ELABORACION, REVISION Y APROBACION

Atentamente

DocuSigned by:
413DA358D32D4B3...

JUAN CARLOS MARTÍNEZ VALDÉS
REPRESENTANTE LEGAL
SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.

DS JCHV DS JAR

Ciudad de México, a 13 de mayo de 202

C. MOISES O. LIMÓN ORTEGA
TITULAR DE LA DIVISIÓN DE SERVICIOS INTEGRALES
DEL INSTITUTO MEXICANO DEL SEGURO SOCIAL
PRESENTE

Juan Carlos Martínez Valdés en mi carácter de representante legal de la empresa Sixsigma Networks México, S.A. de C.V. (KIO), me refiero a su oficio número 09 53 84 6 1CFE / 2022 /004364 de fecha 13 de mayo de 2022 en el cual, en atención a los requerimientos de la Coordinación de Servicios de Infraestructura Tecnológica Institucional de la Dirección de Innovación y Desarrollo Tecnológico quién funge como área requirente/técnica, así como, el resultado de la Investigación de Mercado y de conformidad con la justificación y dictamen de dicha área requirente en términos del artículo 41 penúltimo párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP).

Al respecto, en atención a su petición adjunto la cotización que ratifica los precios ofertados para el "Servicio de Continuidad de la Nube IMSS 2022". Asimismo, manifiesto la aceptación y cumplimiento de todos y cada uno de los requisitos y condiciones establecidos en el Anexo Técnico; Términos y Condiciones con sus respectivos apéndices que integran el requerimiento para la prestación del referido servicio.

Solicitud de cotización para la investigación de Mercado para el "Servicio de Continuidad de la Nube IMSS 2022

Empresa: SIXSIGMA NETWORKS MEXICO, S.A. DE C.V.

Fecha: 13/05/2022

ID del Servicio	Nombre del Servicio	Precio Unitario por Componente de Infraestructura ofertado				Unidad de referencia	Oferta acumulada por Servicio				Oferta acumulada por modalidad					Meses de Servicio	Total por Concepto
		CDP-Prod	CDP-QA	ENP	SDI		CDP-Prod	CDP-QA	ENP	SDI	CDP-Prod	CDP-QA	ENP	SDI	Subtotal		
1	Servidor X86	$11,145.24	$9,120.42	$11,145.24	$8,654.57	Unitario Mensual	52	2	1	335	$579,552.48	$18,240.84	$11,145.24	$2,899,280.95	$3,508,219.51	9	$31,573,975.59
2	Incrementos de Módulos de 1 Procesador con 128 threads X86	$5,720.05	$5,165.25	$5,720.05	$5,720.05	Unitario Mensual	42	2	1	1	$240,242.10	$10,330.50	$5,720.05	$5,720.05	$262,012.70	9	$2,358,114.30

KIONetworks

DIVISIÓN DE CONTRATOS

3	Incremento de 128GB de memoria RAM X86	$52,831.18	$47,603.55	$52,831.18	$52,831.18	Unitario Mensual	12	2	8	1	$633,974.16	$95,207.10	$422,649.44	$52,831.18	$1,204,661.88	9	$10,841,956.92
4	Módulo de Seguridad en Hardware (HSM)	$43,207.82	$43,207.82	N/A	N/A	Unitario Mensual	1	1	N/A	N/A	$43,207.82	$43,207.82	N/A	N/A	$86,415.64	9	$777,740.76
5	Almacenamiento de Datos Individual	$1,734.54	$1,734.54	$1,734.54	$1,734.54	Unitario Mensual	25	1	1	506	$43,363.50	$1,734.54	$1,734.54	$877,677.24	$924,509.82	9	$8,320,588.38
6	Incremento de Almacenamiento de Datos Individual de 100GB	$360.66	$352.06	$360.66	$360.66	Unitario Mensual	3,252	205	1	433	$1,172,866.32	$72,172.30	$360.66	$156,165.78	$1,401,565.06	9	$12,614,085.54
7	Respaldo de Datos Individual	$559.56	$559.56	$559.56	$559.56	Unitario Mensual	81	1	1	17	$45,324.36	$559.56	$559.56	$9,512.52	$55,956.00	9	$503,604.00
8	Unidad de Respaldo en Cintas	$127,904.18	N/A	N/A	N/A	Unitario Mensual	1	N/A	N/A	N/A	$127,904.18	N/A	N/A	N/A	$127,904.18	9	$1,151,137.62
9	Servicio de resguardo de 50 Cintas para la Unidad de Respaldo	$1,436.00	N/A	N/A	N/A	Unitario Mensual	1	N/A	N/A	N/A	$1,436.00	N/A	N/A	N/A	$1,436.00	9	$12,924.00
10	Unidad de almacenamiento de media categoría para aplicaciones de bajo desempeño	N/A	N/A	$113,610.76	N/A	Unitario Mensual	N/A	N/A	2	N/A	N/A	N/A	$227,221.52	N/A	$227,221.52	9	$2,044,993.68
11	Incremento en disco de estado solido 1TB para almacenamiento bajo desempeño	$9,910.81	$9,910.81	$9,910.81	$9,910.81	Unitario Mensual	1	1	1	1	$9,910.81	$9,910.81	$9,910.81	$9,910.81	$39,643.24	9	$356,789.16
12	Incremento en disco FC solido 1TB usable para almacenamiento bajo desempeño	$4,038.05	$4,038.05	N/A	$4,038.05	Unitario Mensual	16	1	N/A	1	$64,608.80	$4,038.05	N/A	$4,038.05	$72,684.90	9	$654,164.10
14	Unidad de respaldo de plataforma abierta	$397,963.95	N/A	$241,453.31	N/A	Unitario Mensual	5	N/A	1	N/A	$1,989,819.75	N/A	$241,453.31	N/A	$2,231,273.06	9	$20,081,457.54
15	Incremento de bloques de 30TB usables en arreglo RAID 5 para unidades de plataforma abierta	$22,038.44	N/A	N/A	N/A	Unitario Mensual	13	N/A	N/A	N/A	$286,499.72	N/A	N/A	N/A	$286,499.72	9	$2,578,497.48

KIONetworks

16	Unidad de Almacenamiento de Datos de alto rendimiento y red SAN	$419,372.77	N/A	N/A	N/A	Unitario Mensual	1	N/A	N/A	N/A	$419,372.77	N/A	N/A	N/A	$419,372.77	9	$3,774,354.93
17	Incremento en discos de estado sólido 1TB para almacenamiento de alto rendimiento	$2,917.07	$2,917.07	$2,917.07	$2,917.07	Unitario Mensual	80	1	1	1	$233,365.60	$2,917.07	$2,917.07	$2,917.07	$242,116.81	9	$2,179,051.29
22	Unidad individual de respaldos (Portátil)	N/A	N/A	N/A	$839.94	Unitario Mensual	N/A	N/A	N/A	505	N/A	N/A	N/A	$424,169.70	$424,169.70	9	$3,817,527.30
23	Sistema Operativo Red Hat Enterprise Linux	$1,162.56	$581.29	$1,162.56	$1,162.56	Unitario Mensual	27	8	1	1	$31,389.12	$4,650.32	$1,162.56	$1,162.56	$38,364.56	9	$345,281.04
24	Sistema Operativo SLES	$1,182.82	$591.42	$1,182.82	$1,182.82	Unitario Mensual	9	2	1	1	$10,645.38	$1,182.84	$1,182.82	$1,182.82	$14,193.86	9	$127,744.74
25	Sistema Operativo Oracle Linux Server	$631.67	$631.67	$631.67	$631.67	Unitario Mensual	1	1	1	1	$631.67	$631.67	$631.67	$631.67	$2,526.68	9	$22,740.12
27	Servidor Virtual RISC SPARC	$88,097.55	N/A	N/A	N/A	Unitario Mensual	16	N/A	N/A	N/A	$1,409,560.80	N/A	N/A	N/A	$1,409,560.80	9	$12,686,047.20
28	Incremento de 1 Procesador Virtual con 128 threads RISC	$3,127.48	N/A	N/A	N/A	Unitario Mensual	11	N/A	N/A	N/A	$34,402.28	N/A	N/A	N/A	$34,402.28	9	$309,620.52
29	Incremento de 32GB de memoria Virtual RAM RISC	$3,650.23	N/A	N/A	N/A	Unitario Mensual	6	N/A	N/A	N/A	$21,901.38	N/A	N/A	N/A	$21,901.38	9	$197,112.42
30	Servidor Virtual X86	$1,947.37	$1,920.42	$1,832.62	N/A	Unitario Mensual	370	110	30	N/A	$720,526.90	$211,246.20	$54,978.60	N/A	$986,751.70	9	$8,880,765.30
31	Incremento Virtualizado Modulos de 1 Procesador Virtual con 8 threads X86	$393.87	$393.87	$393.87	N/A	Unitario Mensual	416	1	20	N/A	$163,849.92	$393.87	$7,877.40	N/A	$172,121.19	9	$1,549,090.71
32	Incremento Virtualizado 8GB de memoria RAM X86	$1,383.80	$1,383.80	$1,383.80	N/A	Unitario Mensual	495	14	12	N/A	$684,981.00	$19,373.20	$16,605.60	N/A	$720,959.80	9	$6,488,638.20
33	Puntos de Acceso a la Nube	N/A	N/A	$203.07	N/A	Unitario Mensual	N/A	N/A	1,322	N/A	N/A	N/A	$268,458.54	N/A	$268,458.54	9	$2,416,126.86
34	Escritorio en la Nube	N/A	N/A	$351.97	N/A	Unitario Mensual	N/A	N/A	955	N/A	N/A	N/A	$336,131.35	N/A	$336,131.35	9	$3,025,182.15
35	Plataforma de Virtualización multi-tecnología	$582,725.30	N/A	$379,967.98	N/A	Unitario Mensual	1	N/A	1	N/A	$582,725.30	N/A	$379,967.98	N/A	$962,693.28	9	$8,664,239.55

DIVISIÓN DE CONTRATOS

KIONetworks

44	Punto Neutro	$638,612.37	N/A	N/A	N/A	Unitario Mensual	1	N/A	N/A	N/A	$638,612.37	N/A	N/A	N/A	$638,612.37	9	$5,747,511.33
53	Conectividad de Enlaces MPLS 5 Gbps redundante activo - activo	$209,069.11	N/A	$209,069.11	$209,069.11	Unitario Mensual	1	N/A	1	1	$209,069.11	N/A	$209,069.11	$209,069.11	$627,207.33	5	$3,136,036.65
68	Conectividad de Enlaces Lan2Lan 100 Mbps redundante activo - activo	N/A	N/A	N/A	$43,691.72	Unitario Mensual	N/A	N/A	N/A	1	N/A	N/A	N/A	$43,691.72	$43,691.72	5	$218,458.60
70	Conectividad de Enlaces Lan2Lan 500 Mbps redundante activo - activo	N/A	N/A	N/A	$96,570.35	Unitario Mensual	N/A	N/A	N/A	1	N/A	N/A	N/A	$96,570.35	$96,570.35	5	$482,851.75
71	Conectividad de Enlaces Lan2Lan 1 Gbps redundante activo - activo	N/A	N/A	N/A	$123,940.54	Unitario Mensual	N/A	N/A	N/A	1	N/A	N/A	N/A	$123,940.54	$123,940.54	5	$619,702.70
72	Conectividad de Enlaces Lan2Lan 3 Gbps redundante activo - activo	N/A	N/A	N/A	$184,067.68	Unitario Mensual	N/A	N/A	N/A	1	N/A	N/A	N/A	$184,067.68	$184,067.68	5	$920,338.40
73	Conectividad de Enlaces Lan2Lan 5 Gbps redundante activo - activo	N/A	N/A	N/A	$221,229.20	Unitario Mensual	N/A	N/A	N/A	1	N/A	N/A	N/A	$221,229.20	$221,229.20	5	$1,106,146.00
74	Conectividad de Enlaces Lan2Lan 10 Gbps redundante activo - activo	N/A	N/A	N/A	$283,366.93	Unitario Mensual	N/A	N/A	N/A	1	N/A	N/A	N/A	$283,366.93	$283,366.93	5	$1,416,834.65
84	Incremento de ancho de banda en Enlaces Lan2Lan 10 Gbps redundante activo - activo	N/A	N/A	N/A	$283,366.93	Unitario Mensual	N/A	N/A	N/A	1	N/A	N/A	N/A	$283,366.93	$283,366.93	5	$1,416,834.65
85	UTM para enlaces de banda ancha hasta 100 Mbps	N/A	N/A	N/A	$3,715.44	Unitario Mensual	N/A	N/A	N/A	1	N/A	N/A	N/A	$3,715.44	$3,715.44	9	$33,438.96
86	UTM para enlaces de banda ancha hasta 10 Gbps	N/A	N/A	$49,399.71	$49,399.71	Unitario Mensual	N/A	N/A	2	1	N/A	N/A	$98,799.42	$49,399.71	$148,199.13	9	$1,333,792.17
87	Acelerador WAN	$6,443.68	N/A	N/A	N/A	Unitario Mensual	1	N/A	N/A	N/A	$6,443.68	N/A	N/A	N/A	$6,443.68	9	$57,993.12
88	Gestor de Optimización WAN	$25,452.55	N/A	N/A	N/A	Unitario Mensual	1	N/A	N/A	N/A	$25,452.55	N/A	N/A	N/A	$25,452.55	9	$229,072.95
89	Balanceador de carga de capas L4-L7	$139,662.59	$105,234.58	N/A	N/A	Unitario Mensual	2	1	N/A	N/A	$279,325.18	$105,234.58	N/A	N/A	$384,559.76	9	$3,461,037.84

KIO Networks

91	Plataforma Nodo de Extensión de Nube Privada - Tamaño grande	N/A	N/A	$794,460.52	N/A	Unitario Mensual	N/A	N/A	1	N/A	N/A	N/A	$794,460.52	N/A	$794,460.52	9	$7,150,144.68
94	Piso Blanco (m2)	$20,633.15	N/A	N/A	N/A	Unitario Mensual	3	N/A	N/A	N/A	$61,899.45	N/A	N/A	N/A	$61,899.45	9	$557,095.05
95	Espacio en Rack	$20,041.71	N/A	N/A	N/A	Unitario Mensual	1	N/A	N/A	N/A	$20,041.71	N/A	N/A	N/A	$20,041.71	9	$180,375.39
108	Subscripciones a Bases de Datos Open Source	$19,070.04	$19,070.04	N/A	N/A	Unitario Mensual	1	1	N/A	N/A	$19,070.04	$19,070.04	N/A	N/A	$38,140.08	9	$343,260.72
110	Java Development Kit	$3,618.05	$3,618.05	N/A	N/A	Unitario Mensual	3	1	N/A	N/A	$10,854.15	$3,618.05	N/A	N/A	$14,472.20	9	$130,249.80
113	Drupal	$4,542.80	$4,542.80	N/A	N/A	Unitario Mensual	1	1	N/A	N/A	$4,542.80	$4,542.80	N/A	N/A	$9,085.60	9	$81,770.40
114	Liferay Enterprise 7/24	$48,946.97	$48,946.97	N/A	$48,946.97	Unitario Mensual	7	1	N/A	1	$342,628.79	$48,946.97	N/A	$48,946.97	$440,522.73	9	$3,964,704.57
115	Alfresco	$28,145.01	$28,145.01	N/A	$28,145.01	Unitario Mensual	4	1	N/A	1	$112,580.04	$28,145.01	N/A	$28,145.01	$168,870.05	9	$1,519,830.54
118	Tuxedo	$21,264.15	$21,264.15	N/A	N/A	Unitario Mensual	1	1	N/A	N/A	$21,264.15	$21,264.15	N/A	N/A	$42,528.30	9	$382,754.70
119	GlassFish	$15,076.39	$15,076.39	N/A	N/A	Unitario Mensual	8	1	N/A	N/A	$120,611.12	$15,076.39	N/A	N/A	$135,687.51	9	$1,221,187.59
120	Apache Tomcat	$238.38	$238.38	N/A	N/A	Unitario Mensual	1	1	N/A	N/A	$238.38	$238.38	N/A	N/A	$476.76	9	$4,290.84
121	Apache HTTPD	$202.01	$202.01	N/A	N/A	Unitario Mensual	63	34	N/A	N/A	$12,726.63	$6,868.34	N/A	N/A	$19,594.97	9	$176,354.73
122	Servicio de correo electrónico.	$6.53	N/A	N/A	N/A	Unitario Mensual	92,051	N/A	N/A	N/A	$600,770.85	N/A	N/A	N/A	$600,770.85	9	$5,406,937.66
126	Firewall	$92,839.76	N/A	$97,726.06	$97,726.06	Unitario Mensual	6	N/A	1	1	$557,038.54	N/A	$97,726.06	$97,726.06	$752,490.66	9	$6,772,415.96
127	IPS	$229,361.61	N/A	N/A	N/A	Unitario Mensual	2	N/A	N/A	N/A	$458,723.21	N/A	N/A	N/A	$458,723.21	5	$2,293,616.07
128	Anti-Denegación de Servicios (DDoS)	$201,627.13	N/A	N/A	N/A	Unitario Mensual	2	N/A	N/A	N/A	$403,254.25	N/A	N/A	N/A	$403,254.25	5	$2,016,271.26
130	Gestión Unificada de Amenazas (UTM)	$31,117.47	N/A	N/A	$31,117.47	Unitario Mensual	4	N/A	N/A	1	$124,469.88	N/A	N/A	$31,117.47	$155,587.35	5	$777,936.75
134	Firewall Especializado en Servicios Web (WAF)	$211,656.08	N/A	N/A	N/A	Unitario Mensual	2	N/A	N/A	N/A	$423,312.16	N/A	N/A	N/A	$423,312.16	5	$2,116,560.78
136	Nodo de red con UTP	$110.97	N/A	$350.84	N/A	Unitario por servicio	22	N/A	607	N/A	$2,441.34	N/A	$212,959.88	N/A	$215,401.22	9	$1,938,610.98

DIVISIÓN DE CONTRATOS

KIONetworks

137	Nodo de red con Fibra Optica	$474.89	N/A	$474.89	N/A	Unitario por servicio	N/A	N/A	64	N/A	N/A	N/A	$30,392.96	N/A	$30,392.96	9	$273,536.64
139	Switch de 10G de core	N/A	N/A	$9,123.05	$9,123.05	Unitario Mensual	N/A	N/A	14	5	N/A	N/A	$127,722.70	$45,615.25	$173,337.95	9	$1,560,041.55
140	Switch de 10 de distribución	N/A	N/A	$3,560.92	$3,560.92	Unitario Mensual	N/A	N/A	70	10	N/A	N/A	$249,264.40	$35,609.20	$284,873.60	9	$2,563,862.40
142	UTM para enlaces a Red Nacional para Impulso de la Banda Ancha (NIBA) de 100 Mbps	N/A	N/A	N/A	$3,715.44	Unitario por servicio	N/A	N/A	N/A	1	N/A	N/A	N/A	$3,715.44	$3,715.44	9	$33,438.96
143	UTM para enlaces a Red Nacional para Impulso de la Banda Ancha (NIBA) de 1 Gbps	N/A	N/A	N/A	$42,938.13	Unitario por servicio	N/A	N/A	N/A	1	N/A	N/A	N/A	$42,938.13	$42,938.13	9	$386,443.17
144	UTM para enlaces a Red Nacional para Impulso de la Banda Ancha (NIBA) de 10 Gbps	N/A	N/A	N/A	$58,444.20	Unitario por servicio	N/A	N/A	N/A	1	N/A	N/A	N/A	$58,444.20	$58,444.20	9	$525,997.80
161	Enlaces Internet 100 Mbps redundante activo - activo	N/A	N/A	$85,971.43	$85,971.43	Unitario Mensual	N/A	N/A	1	4	N/A	N/A	$85,971.43	$343,885.72	$429,857.15	5	$2,149,285.75
178	Sistema de Almacenamiento de datos en RAID5 de 12TB con capacidad de crecimiento hasta 32TB	$56,281.22	N/A	N/A	N/A	Unitario Mensual	74	N/A	N/A	N/A	$4,164,810.28	N/A	N/A	N/A	$4,164,810.28	9	$37,483,292.52
179	Incremento de almacenamiento de datos en RAID5 por unidad de TB	$9,430.18	N/A	N/A	N/A	Unitario Mensual	1	N/A	N/A	N/A	$9,430.18	N/A	N/A	N/A	$9,430.18	9	$84,871.62
180	Solución para el cumplimiento WCAG	$305,146.18	N/A	N/A	N/A	Unitario Mensual	1	N/A	N/A	N/A	$305,146.18	N/A	N/A	N/A	$305,146.18	8	$2,441,169.44
																Subtotal A	**$253,069,909.49**
																IVA	**$40,491,185.52**
																TOTAL A	**$293,561,095.01**

CDP - Centro de Datos Primario (Ambientes Productivos y no Productivos)

ENP - Extensión de Nube Privada (ATOM)

SDI - Servicios desplegados en Instalaciones designadas por el Instituto

KIO Networks

Servicios de soporte recurrentes

ID del Servicio	Nombre del Servicio	Precio unitario	Unidad de referencia	Unidades de consumo para evaluacion	Subtotal B
181	Servicio deSoporte para la Integridad de la Nube IMSS	$2,000,000.00	Unitario Mensual	9 meses	$18,000,000.00
182	Servicio deSoporte para la Operación de la Seguridad de la Nube IMSS	$1,250,000.00	Unitario Mensual	9 meses	$11,250,000.00
183	Servicio deSoporte de Servicio de Continuidad a la Operación y Soporte de la Nube IMSS	$2,000,000.00	Unitario Mensual	9 meses	$18,000,000.00
				Subtotal B	**$47,250,000.00**
				IVA	**$7,560,000.00**
				TOTAL B	**$54,810,000.00**

El posible proveedor deberá tomar las medidas necesarias para garantizar la continuidad del servicio actual, mismo que finaliza el 31 de diciembre de 2022
El costo de este concepto será reflejado en la propuesta económica del posible proveedor bajo el rubro "migración de centros de datos".
El número de días de migración ofertado por el Licitante será un dato relevante en la evaluación considerando el criterio de aceptación que se describe a continuación:

ANEXOS
DIVISIÓN DE CONTRATOS

KIO Networks

ID del Servicio	Nombre del Servicio	Costo Total migracion	Número de días naturales de migración ofertados	Precio por día de migracion	Subtotal C	IVA	Total C
184	Migración de centro de datos	$1.00	1	$1.00	**$1.00**	**$0.16**	**$1.16**

Cuadro Resumen de la propuesta económica del posible proveedor:			
Concepto	Subtotal	IVA	Total
Costo unitario de servicios BCFs (Subtotal A)	$253,069,909.49	$40,491,185.52	$293,561,095.01
Servicios de soporte y recurrentes (Subtotal B)	$47,250,000.00	$7,560,000.00	$54,810,000.00
Migración de centro de datos (Subtotal C)	$1.00	$0.16	$1.16
Total	$300,319,910.49	$48,051,185.68	$348,371,096.17

El criterio para considerar concluida la migración desde el Centro de Datos actual hacia el Centro de Datos ofertado, será en el momento en que se encuentren los servicios descritos anteriormente activos y operando en la infraestructura propuesta por el Licitante, e interactuando con el ecosistema tecnológico institucional, esto es; con los ambientes operativos digitales productivos y no productivos instalados en los diferentes centros de datos IMSS y del Gobierno Federal así como organismos con los que interactúa el Instituto tales como SAT, RENAPO, INFONAVIT, BANCO DE MÉXICO, PROCESAR, CONSAR, BANCOS Y AFORES, entre otros, validados de conformidad por el personal que el Instituto designe (áreas de telecomunicaciones y seguridad informática, infraestructura tecnológica, desarrollo, monitoreo así como el personal de las direcciones normativas que hacen uso de los servicios en los casos que aplique).

Atentamente

JUAN CARLOS MARTÍNEZ VALDÉS
REPRESENTANTE LEGAL
SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.

KIO Networks

GOBIERNO DE MÉXICO

IMSS

DIRECCIÓN DE ADMINISTRACIÓN
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Bienes y Servicios
División de Servicios Integrales

Of N° 09 53 84 61 1CFE/2022/004453

Ciudad de México, a 17 de mayo de 2022

SIXSIGMA NETWORKS MEXICO, S.A. DE C.V.
Prolongación Paseo de la Reforma No 5287,
Colonia Cuajimalpa, Cuajimalpa de Morelos, C.P.
05000, Ciudad de México.
Presente

At´n Juan Carlos Martínez Valdés
Representante Legal

Con relación al procedimiento de Adjudicación Directa Internacional bajo la Cobertura de Tratados número No. AA-050GYR988-E20-2022, para la contratación del "Servicio de Continuidad de la Nube IMSS 2022"; a la investigación de mercado y justificación realizada por la Coordinación de Servicios de Infraestructura Tecnológica Institucional de la Dirección de Innovación y Desarrollo Tecnológico, mediante la cual dictaminó como procedente la excepción a la Licitación Pública para llevar a cabo la contratación del servicio a través de una adjudicación directa, remitida con el oficio No. 0952176K5300/2022000482 recibido el 29 de abril de 2022, con fundamento en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos, 3 fracción IX, 25 primer párrafo, 26 fraccion III, 40, 41 fracción II, y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP); así como 71 y 85 de su Reglamento, se le notifica la adjudicación del contrato abierto relativo al servicio, ya que cumplió técnica, legal, administrativa y económica con lo requerido para la prestación del servicio, de conformidad con la ratificación de los precios ofertados y el importe mínimo y máximo de su propuesta económica como se describen a continuación:

Monto Mínimo	Monto Máximo
$139,348,438.46 (Ciento treinta y nueve millones trescientos cuarenta y ocho mil cuatrocientos treinta y ocho pesos 46/100 M.N.)	$348,371,096.17 (Trescientos cuarenta y ocho millones trescientos setenta y un mil noventa y seis pesos 17/100 M.N.)

Importes incluyen el Impuesto al Valor Agregado (I.V.A.)

La vigencia del servicio será a partir del día siguiente de la presente notificación de la adjudicación y hasta el 31 de diciembre de 2022.

RECIBIDO

17 MAYO 2022

Nombre:

Firma:

11:00 hrs

1

Av. Durango No. 291, Piso 4, Col. Roma Norte, Alcaldía Cuauhtémoc, C. P. 06700, Ciudad de México
Tel: 55 5628 1900 Ext. 34761 www.imss.gob.mx

2022 Ricardo Flores Magón
Año de

ANEXOS
DIVISIÓN DE CONTRATOS

Se precisa que con fundamento en lo dispuesto por el artículo 37, penúltimo párrafo, y 46, primer párrafo, de la LAASSP, con la presente notificación de adjudicación, su representada se obliga a suscribir el contrato que se derive conforme a lo establecido en la Solicitud de Cotización, en la "descripción de los servicios objeto del procedimiento de contratación y especificaciones técnicas de los mismos", "plazos y condiciones de entrega de los bienes" y el "requerimiento del área" establecidos en el Anexo Técnico, así como en los Términos y condiciones del servicio.

Para la suscripción del contrato es necesario que a más tardar el día hábil siguiente a la recepción del presente oficio de adjudicación entregue la documentación correspondiente para la formalización del citado instrumento jurídico al Titular de la División de Contratos, cuya oficina se encuentra ubicada en Durango 291, décimo piso, Colonia Roma Norte, Código Postal 06700, Demarcación Cuauhtémoc, Ciudad de México, conforme a lo siguiente:

a. Acta constitutiva y, en su caso, sus respectivas modificaciones, inscritas en el Registro Público del Comercio.
b. Poder notarial del representante legal que firmará el contrato.
c. Identificación oficial vigente y con fotografía del representante legal.
d. Registro Patronal.
e. Cédula de Registro Federal de Contribuyentes.
f. Comprobante de domicilio con vigencia no mayor a 3 meses.
g. 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.
h. 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.

El IMSS se reserva el derecho de firmar el contrato si no presenta Opinión favorable SAT e IMSS documentos indispensable para la firma del contrato, toda vez que en caso de no presentarlos se procederá a informar al Órgano Interno de Control la no formalización del contrato por causas imputables al proveedor para que determine, en su caso, la sanción correspondiente.

i. Opinión en la que conste que se encuentra al corriente del cumplimiento de obligaciones en materia de aportaciones patronales y entero de descuentos del Instituto del Fondo Nacional de la Vivienda para los Trabajadores a la firma del contrato emitida por el INFONAVIT, en términos del artículo 32-D del Código Fiscal de la Federación y ACUERDO del H. Consejo de Administración del Instituto del Fondo Nacional de la Vivienda para los Trabajadores por el

Durango No. 291, Piso 6, Col. Roma Norte, Alcaldía Cuauhtémoc, C. P. 06700, Ciudad de México
Tel. 5726 7200 Ext. 14261. www.imss.gob.mx

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 DOF el 28 de junio de 2017.

j. Escrito en el que el particular manifieste bajo protesta de decir verdad que de conformidad con la fracción IX del artículo 49 de la Ley General de Responsabilidades Administrativas, no desempeña empleo, cargo o comisión en el servicio público, en su caso, que, a pesar de desempeñarlo, con la formalización del contrato correspondiente no se actualiza un Conflicto de Interés. En caso de que el participante adjudicado sea persona moral, dichas deberán presentarse respecto a los socios o accionistas que ejerzan control sobre la sociedad. Dicha manifestación se hará del conocimiento del Órgano Interno de Control, previo a la celebración del acto en cuestión.

Para efectos de la referida Ley se entiende que un socio o accionista ejerce control sobre una sociedad cuando sean administradores o formen parte del consejo de administración, o bien conjunta o separadamente, directa o indirectamente, mantengan la titularidad de derechos que permitan ejercer el voto respecto de más del cincuenta por ciento del capital, tengan poder decisorio en sus asambleas, estén en posibilidades de nombrar a la mayoría de los miembros de su órgano de administración o por cualquier otro medio tengan facultades de tomar las decisiones fundamentales de dichas personas morales.

Para efecto de que el área contratante esté en condiciones de incorporar a CompraNet los datos relativos al contrato que se derive de este procedimiento de contratación, la empresa responsable debe estar inscrito y mantener actualizada su información en el Registro Único de Proveedores y Contratistas (RUPC) de CompraNet, de conformidad y para los efectos de lo establecido en las disposiciones 18 y 19 del Acuerdo por el que se establecen las disposiciones que deberán observar para la utilización del Sistema Electrónico de Información Pública Gubernamental denominado CompraNet, publicado en el Diario Oficial de la Federación el 28 de junio de 2011.

Asimismo, deberá entregar en la División de Contratos, a más tardar dentro de los 10 días naturales siguientes a la firma del contrato, la garantía de cumplimiento mediante fianza expedida por afianzadora debidamente constituida en términos de la Ley de Instituciones de Seguros y de Fianzas, en la moneda de la proposición y por el 10% del importe máximo total del contrato a favor del Instituto Mexicano del Seguro Social.

ANEXOS
DIVISIÓN DE CONTRATOS

Fecha para la formalización del contrato	Horario	Dirección de la División de Contratos
Dentro de los quince días naturales posteriores a la presente notificación	9:00 hrs a 18:00hrs	Durango 291, décimo piso, Colonia Roma Norte, Código Postal 06700, Demarcación Cuauhtémoc, Ciudad de México.

En caso de que el proveedor hubiera entregado toda la documentación requerida, podrá formalizar el contrato con anticipación a la fecha señalada, previa solicitud del proveedor y autorización de la División de Contratos.

Lo anterior se comunica de conformidad con el artículo 2 fracción I del Reglamento de la LAASSP, numeral 4.2.4.1.3 del Manual Administrativo de aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como el numeral 5.3.8 inciso a) de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Prestación de Servicios del Instituto Mexicano del Seguro Social.

Sin otro particular, le envío saludos cordiales.

Atentamente

Moises O. Limón Ortega
Titular de la División

C.c.p. **Mtro. Aunard Agustín de la Rocha Waite**, Titular de Coordinación de Adquisición de Bienes y Contratación de Servicios.- Para su conocimiento (*)
C.P. Elvia Ascencio Millán.- Titular de la Coordinación Técnica de Bienes y Servicios.- Mismo Fin (*)
Ing. Eduardo Oropeza Ortiz.- Titular de la Coordinación de Servicios de Infraestructura Tecnológica Institucional adscrito a la DIDT.- Mismo Fin (*)

(*) Copia enviada mediante el Sistema Institucional de Control de Gestión de Correspondencia.

Elaboró: OMMV

IMSS	INSTITUTO MEXICANO DEL SEGURO SOCIAL DIRECCIÓN DE ADMINISTRACIÓN UNIDAD DE ADQUISICIONES COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS	Contrato Número S2M0117

ANEXO 3 (TRES)

"DOCUMENTO DE DESIGNACIÓN DE ADMINISTRADOR DEL CONTRATO"

EL PRESENTE ANEXO CONSTA DE **02** HOJAS INCLUYENDO ESTA CARÁTULA

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

Of. N° 09 52 17 GK 5300/2022000263

Ciudad de México, a 19 de abril de 2022

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 Nube IMSS 2022"***.

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, C. Ing. Eduardo Oropeza Ortiz, con cuenta de correo electrónico: eduardo.oropeza@imss.gob.mx y teléfono 5238-2700, extensión 12356, 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 4.24.6 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 emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal"*, publicado en el Diario Oficial de la Federación el 06 de septiembre de 2021.

Sin otro particular por el momento, hago propicia la ocasión para enviarles un cordial saludo.

Atentamente,

Ing. Eduardo Oropeza Ortiz
Coordinador de Servicios de Infraestructura
Tecnológica Institucional adscrito a la DIDT

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO