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 Soporte Técnico y Operación de la Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube de IMSS y DRP, que celebran por una parte, el **INSTITUTO MEXICANO DEL SEGURO SOCIAL**, que en lo sucesivo se denominará **"EL INSTITUTO"**, representado en este acto por el **C. ALBERTO FLAVIO BALDERAS HERNÁNDEZ**, en su carácter de Apoderado Legal, y por la otra parte el **INSTITUTO POTOSINO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA, A.C.**, en lo sucesivo **"EL IPICYT"**, representada por el **C. LUIS ANTONIO SALAZAR OLIVO**, en su carácter de Representante Legal, y a quienes en forma conjunta se les denominará **"LAS PARTES"**, al tenor de las Declaraciones y Cláusulas siguientes:

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

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

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

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

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

I.4.- El C. Eduardo Oropeza Ortiz, Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional adscrita a la Dirección de Innovación y Desarrollo Tecnológico de **"EL INSTITUTO"**, funge como Administrador del Contrato, responsable de dar seguimiento y verificar el cumplimiento de los derechos y obligaciones establecidos en este instrumento jurídico.

I.5.- Para el cumplimiento de sus funciones y la realización de sus actividades se requiere de la prestación del Servicio de Soporte Técnico y Operación de la Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube de IMSS y DRP, solicitado por la Coordinación de Sistemas de Infraestructura Tecnológica Institucional.

I.6.- Para cubrir las erogaciones que se deriven del presente contrato, cuenta con los recursos disponibles suficientes, no comprometidos, en la cuenta número 42061506 de conformidad con el Dictamen de Disponibilidad Presupuestal Previo con número de folio 0000002733-2020, emitido por la Titular de la División de Control y Seguimiento al Gasto de Operación de fecha 25 de noviembre de 2019, mismo que se agrega al **Anexo 1 (uno)** al presente contrato.

Los recursos presupuestarios a ejercer con motivo del presente instrumento jurídico, quedan sujetos para fines de ejecución y pago, a la disponibilidad presupuestaria con que cuente **"EL INSTITUTO"**, conforme al Presupuesto de Egresos de la Federación que apruebe la H. Cámara de Diputados del Congreso de la Unión, sin responsabilidad alguna para **"EL INSTITUTO"**.

I.7.- Con fecha 24 de diciembre de 2019, la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos, a través de la División de Contratación de Activos y Logística mediante oficio número 09 53 84 61 1CFJ/10236/2019, notificó a **"EL IPICYT"** la adjudicación del procedimiento de Adjudicación Directa número **EPO-050GYR019-N378-2019**, con fundamento en lo dispuesto en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos, 1 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 4° de su Reglamento y demás disposiciones aplicables en la materia, como se detalla en el **Anexo 2 (dos)**, del presente instrumento jurídico.

I.8.- En caso de discrepancia entre el contenido en 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 IPICYT" declara, por conducto de su Representante Legal, que:

II.1.- Es una Asociación Civil constituida de conformidad con las leyes de los Estados Unidos Mexicanos, según consta en la Escritura Pública número 1,663 de fecha 24 de noviembre de 2000, pasada ante la fe del Licenciado Leopoldo de la Garza Marroquín, Titular de la Notaría Pública número 33, en ejercicio en el Primer Distrito Judicial del Estado de San Luis Potosí, inscrita en el Registro Público de la Propiedad y de Comercio de la misma Entidad, bajo la inscripción número 34151 a fojas 267 del tomo 486.

II.2.- El C. Luis Antonio Salazar Olivo, acredita su personalidad en términos de la Escritura Pública número 625 de fecha 12 de marzo de 2019, pasada ante la fe del Licenciado Miguel Martínez Vega, Titular de la Notaría Pública número 14 de San Luis Potosí, e inscrita en el Instituto Registral y Catastral de la misma Entidad bajo el folio AC1-20535 mediante la cual se protocolizó su nombramiento como Director General de **"EL IPICYT"**; a través del oficio número A0000/084/2019, de fecha 08 de febrero de 2019, y manifiesta bajo protesta de decir verdad que las facultades que le fueron conferidas no le han sido revocadas, modificadas ni restringidas en forma alguna.

II.3.- Su objeto social conforme a sus Estatutos consiste, entre otros, en brindar apoyo a la industria y a los sectores público y social mediante servicios, asesorías, consultorías y la generación de desarrollos tecnológicos.

II.4.- Cuenta con el Registro Federal de Contribuyentes número: **IPI001124PX5**.

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 2.1.31 y 2.1.39 de la Resolución Miscelánea Fiscal para 2020, publicada el 28 de diciembre de 2019 en el Diario Oficial de la Federación, del cual presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

II.6.- 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

II.7.- 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.8.- 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 Camino a la Presa San José número 2055, Colonia Lomas 4ª Sección, Código Postal 78216, San Luis Potosí, San Luis Potosí, teléfono (444) 834-2000 ext. 2101, correo electrónico: [redacted]

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 IPICYT" se obliga a prestar el Servicio de Soporte Técnico y Operación de la Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube de IMSS y DRP, 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 del procedimiento del cual deriva el presente contrato.

SEGUNDA.- IMPORTE DEL CONTRATO.- El importe del presente contrato es por la cantidad mínima de **$20,000,000.00 (VEINTE MILLONES DE PESOS 00/100 M.N.)**, incluye el Impuesto

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

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

al Valor Agregado (I.V.A.), y por la cantidad máxima de **$50,000,000.00 (CINCUENTA MILLONES DE PESOS 00/100 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.- El pago será de manera mensual para los servicios recurrentes, por evento para los que sean solicitados a discreción de **"EL INSTITUTO"** y por única ocasión, para los servicios que están planificados como única vez en la vida del presente contrato, de conformidad con lo establecido en los Términos y Condiciones, que se agregan al presente contrato en el **Anexo 1 (uno)**.

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

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

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

"EL IPICYT" expedirá sus facturas en el esquema de facturación electrónica CFDI (Comprobantes Fiscales Digitales por Internet). La recepción de los CFDI será a través del Portal de Servicios a Proveedores, y deberán ser proporcionadas en su formato XML. La validez de los mismos será determinada durante la carga y únicamente los CFDI físicamente válidos serán procedentes para pago. **"EL IPICYT"** deberá proporcionar al administrador del contrato una representación impresa de la misma que cumpla con las especificaciones normadas por el Servicio de Administración Tributaria (SAT). La representación impresa por sí misma no será sustento para pago si no se hace la carga del XML del cual se originó, o si la misma no es una representación fiel del XML origen.

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

El pago se realizará en pesos mexicanos, en los plazos normados por la Dirección de Finanzas en el "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos", sin que éstos rebasen los 20 (veinte) días naturales posteriores a aquel en que **"EL IPICYT"** presente en la División de Trámite de Erogaciones, de **"EL INSTITUTO"** ubicada en calle Gobernador Tiburcio Montiel número 15, Colonia San Miguel Chapultepec, Código Postal 11850, Demarcación Territorial Miguel Hidalgo en la Ciudad de México, en días y horas hábiles.

El pago de los servicios quedará condicionado proporcionalmente al pago que **"EL IPICYT"** deba efectuar por concepto de deducciones.

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

a) **"EL IPICYT"** entregará el CFDI a la Coordinación de Servicios Administrativos de la Dirección de Innovación y Desarrollo Tecnológico (DIDT).
b) La Coordinación de Servicios Administrativos enviará el CFDI a la Coordinación de Sistemas de Infraestructura Tecnológica Institucional para su trámite en términos del presente contrato.
c) La Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI) enviará al respectivo administrador del contrato, el citado CFDI con la petición de que proceda a la validación de los servicios comprendidos en el mismo, en su caso, emita la aceptación a entera satisfacción de los servicios.
d) Los administradores del contrato integrarán los respectivos sustentos documentales incluyendo los resultados del cálculo de las métricas de servicio establecidos en el Anexo Técnico, integrado como **Anexo 1 (uno)** al presente contrato, para la aplicación de deducciones conducentes enviándola a la Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI).
e) La Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI) valida y enviará la documentación completa a la Coordinación de Servicios Administrativos para la gestión de pago.
f) La Coordinación de Servicios Administrativos entregará el CFDI a **"EL IPICYT"**.
g) **"EL IPICYT"** deberá ingresar su CFDI y documentación al área de Trámite de Erogaciones para los trámites correspondientes.

"EL IPICYT" deberá expedir sus CFDI, en el esquema de facturación electrónica, con las especificaciones normadas por el Servicio de Administración Tributaria (SAT) a nombre del

Instituto Mexicano del Seguro Social, con Registro Federal de Contribuyentes IMS421231I45, domicilio en Avenida Paseo de la Reforma número 476, Colonia Juárez, Código Postal 06600, Demarcación Territorial Cuauhtémoc, en la Ciudad de México.

"EL IPICYT", 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 IPICYT"** 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 IPICYT"** proporcionará con oportunidad su número de cuenta, CLABE, banco y sucursal, a menos que **"EL IPICYT"** 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 IPICYT"** 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".

"EL IPICYT" 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 IPICYT" 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.

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

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

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

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

Para que **"EL IPICYT"** pueda celebrar un contrato de cesión de derechos de cobro, deberá notificarlo por escrito a **"EL INSTITUTO"** con un mínimo de 5 días naturales anteriores a la fecha de pago programada; el Administrador del Contrato o, en su caso, el Titular del Área Requirente, deberá entregar los documentos sustantivos de dicha cesión al área responsable de 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".

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 IPICYT"** 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 IPICYT"** presente su CFDI o factura con errores o deficiencias, **"EL INSTITUTO"** dentro de los 3 (tres) días hábiles siguientes a la recepción de la misma, indicará por escrito a **"EL IPICYT"** las deficiencias o errores que deberá corregir. El periodo que transcurra a partir de la entrega del citado escrito y hasta que **"EL IPICYT"** 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, previa solicitud por escrito acompañada de los documentos siguientes:

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

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

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

El pago del servicio quedará condicionado proporcionalmente al pago que **"EL IPICYT"** deba efectuar por concepto de deducciones. **"EL INSTITUTO"** realizará las retenciones correspondientes sobre el CFDI que se presente para pago.

CUARTA.- PLAZO, LUGAR Y CONDICIONES DE LA PRESTACIÓN DEL SERVICIO.- "EL IPICYT" 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 y de acuerdo con lo siguiente:

PLAZO DE LA PRESTACIÓN DEL SERVICIO.- El servicio se proporcionará a partir del 01 de enero y hasta el 29 de febrero de 2020.

La definición de la programación, implementación y desarrollo de los servicios se establece en el Anexo Técnico, integrado como **Anexo 1 (uno)** al presente contrato.

LUGAR DE LA PRESTACIÓN DEL SERVICIO.- "EL IPICYT" se obliga a prestar el servicio en los las ubicaciones señaladas en los Términos y Condiciones, integrados como **Anexo 1 (uno)** al presente contrato o en las nuevas ubicaciones que **"EL INSTITUTO"** defina durante la vida del presente contrato, ya sea incrementando o sustituyendo algunas de las ubicaciones existentes, con objeto de acondicionar los servicios necesarios para su adecuado funcionamiento.

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

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 01 de enero y hasta el 29 de febrero de 2020.

SEXTA.- TRANSFERENCIA DE DERECHOS DE COBRO.- "EL IPICYT" 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.

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

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

"EL IPICYT" 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 IPICYT"** se origina un retraso en el pago, no procederá el pago de los gastos financieros.

SÉPTIMA.- RESPONSABILIDAD.- "EL IPICYT" 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.

OCTAVA.- CONTRIBUCIONES.- Los impuestos y/o derechos que procedan con motivo del servicio objeto del presente contrato, serán pagados por **"EL IPICYT"** 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 IPICYT", 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 IPICYT" 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 IPICYT" 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 IPICYT"** manifiesta en este acto bajo protesta de decir verdad, no encontrarse en ninguno de los supuestos de infracción a la Ley Federal del Derecho de Autor, ni a la Ley de la Propiedad Industrial.

En caso de que sobreviniera alguna reclamación en contra de **"EL INSTITUTO"** por cualquiera de las causas antes mencionadas, la única obligación de éste será la de dar aviso en el domicilio previsto en este instrumento jurídico a **"EL IPICYT"**, 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.

Asimismo, **"EL IPICYT"** deberá cumplir con lo señalado en el numeral 9 de los Términos y Condiciones que se integran al presente contrato, como **Anexo 1 (uno)**.

DÉCIMA.- DEDUCCIONES.- "EL IPICYT", por la entrega parcial o deficiente del servicio, se hará acreedor a las deducciones conforme los conceptos y porcentajes señalados en el numeral 23 de Anexo Técnico que se integran en el **Anexo 1 (uno)** del presente contrato.

El administrador del presente contrato será responsable del cálculo, aplicación y seguimiento de las deducciones.

En su caso, se podrá proceder a la rescisión del contrato.

DÉCIMA PRIMERA.- TERMINACIÓN ANTICIPADA DEL CONTRATO.- "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 SEGUNDA.- SUSPENSIÓN DEL SERVICIO.- En caso fortuito o fuerza mayor, bajo su responsabilidad, **"EL INSTITUTO"** podrá suspender la prestación del servicio, 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 IPICYT"** los gastos no recuperables, 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 TERCERA.- 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 IPICYT"** incurra en cualquiera de las causales que se señalan a continuación:

1. Cuando incurra en falta de veracidad total o parcial respecto a la información proporcionada para la celebración del presente contrato.

2. Cuando incumpla, total o parcialmente, con cualesquiera de las obligaciones establecidas en el presente contrato y sus anexos.

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. Cuando de manera reiterativa y constante, **"EL IPICYT"** sea sancionado por parte de **"EL INSTITUTO"** con deducciones sobre el mismo concepto de los servicios que proporciona.

6. Si **"EL IPICYT"** no permite a **"EL INSTITUTO"** la administración y verificación a que se refiere la cláusula correspondiente del presente contrato.

DÉCIMA CUARTA.- RESCISIÓN ADMINISTRATIVA DEL CONTRATO.- "EL INSTITUTO" podrá rescindir administrativamente el presente contrato en cualquier momento, cuando **"EL IPICYT"** incurra en incumplimiento de cualquiera de las obligaciones a su cargo, de conformidad con el procedimiento siguiente:

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

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

c) La determinación de dar o no por rescindido administrativamente el presente contrato, deberá ser debidamente fundada, motivada y comunicada por escrito a **"EL IPICYT"** dentro de los 15 (quince) días hábiles siguientes, al vencimiento del plazo señalado en el inciso a), de esta Cláusula.

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, 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 IPICYT"** 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 IPICYT"** 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.

"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 IPICYT"**, un nuevo plazo para el cumplimiento de aquellas obligaciones que se hubiesen dejado de cumplir, a efecto de que **"EL IPICYT"** subsane el incumplimiento que hubiere motivado el inicio del procedimiento de rescisión. Lo anterior se llevará a cabo a través de un convenio modificatorio.

DÉCIMA QUINTA.- RELACIÓN LABORAL.- "LAS PARTES" convienen en que **"EL INSTITUTO"** no adquiere ninguna obligación de carácter laboral para con **"EL IPICYT"** 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 IPICYT"**.

Por lo anterior, no se le considerará a **"EL INSTITUTO"** como patrón, ni aún substituto, y **"EL IPICYT"** 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 IPICYT" 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 SEXTA.- 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 IPICYT"** y sea propiedad exclusiva de **"EL INSTITUTO"**.

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

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

Por lo expuesto, **"EL IPICYT"** 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, respetando el manejo confidencial de la información.

2) Toda la información a que tenga acceso el personal que **"EL IPICYT"** designe para la prestación de los servicios materia del presente contrato, es considerada de carácter confidencial, por lo que **"EL IPICYT"** deberá garantizar que por ningún motivo se viole ninguno de los siguientes acuerdos:

    a. La información de **"EL INSTITUTO"** y a la cual tenga acceso el personal de **"EL IPICYT"**, no deberá ser copiada o respaldada en ninguno de los equipos del personal de **"EL IPICYT"**sin autorización previa del Administrador del Contrato dentro del ámbito de su competencia.
    b. El acceso a la información de **"EL INSTITUTO"** por parte del personal de **"EL IPICYT"**, 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 IPICYT"**.

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" 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.

d) Aquella cuya revelación haya sido aprobada previamente por escrito.

e) La que de acuerdo a la Ley u orden judicial o administrativa, deba ser suministrada a terceras personas.

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

DÉCIMA SÉPTIMA.- MODIFICACIONES.- "EL INSTITUTO" podrá celebrar por escrito Convenio Modificatorio, al presente contrato dentro de la vigencia del mismo.

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 IPICYT"** 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.

DÉCIMA OCTAVA.- ADMINISTRACIÓN Y VERIFICACIÓN.- El C. Eduardo Oropeza Ortiz, Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional adscrita a la Dirección de Innovación y Desarrollo Tecnológico 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)**.

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.

DÉCIMA NOVENA.- PROCEDIMIENTO DE CONCILIACIÓN.- En cualquier momento durante la vigencia del presente Contrato, **"EL IPICYT"** o **"EL INSTITUTO"** podrán presentar ante el Órgano Interno de Control en **"EL INSTITUTO"** solicitud de conciliación por desavenencias, derivadas del presente instrumento jurídico.

VIGÉSIMA.- 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, Términos y Condiciones"

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

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

Anexo 2 (dos) "Propuesta Técnica, Propuesta Económica y Oficio de Notificación de Adjudicación"

Anexo 3 (tres) "Documento de designación de Administrador del Contrato"

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

Previa lectura y debidamente enteradas **"LAS PARTES"** del contenido, alcance y fuerza legal del presente contrato, en virtud de que se ajusta a la expresión de su libre voluntad y que su consentimiento no se encuentra afectado por dolo, error, mala fe, ni otros vicios de la voluntad, lo firman y ratifican en todas sus partes, por quintuplicado, en la Ciudad de México, el **08 de enero de 2020**, quedando un ejemplar en poder de **"EL IPICYT"** y los restantes en poder de **"EL INSTITUTO"**.

"EL INSTITUTO" **INSTITUTO MEXICANO DEL SEGURO SOCIAL**	**"EL IPICYT"** **INSTITUTO POTOSINO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA, A.C.**
C. ALBERTO FLAVIO BALDERAS HERNÁNDEZ Apoderado Legal	**C. LUIS ANTONIO SALAZAR OLIVO** Representante Legal

ADMINISTRADOR DEL CONTRATO

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

BJN/CPRD/LMLR/XPMM

SIN TEXTO

	INSTITUTO MEXICANO DEL SEGURO SOCIAL **DIRECCIÓN DE ADMINISTRACIÓN** **UNIDAD DE ADQUISICIONES E INFRAESTRUCTURA** **COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS** **COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS**	**Contrato Número P0M0017**

ANEXO 1 (UNO)

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

ANEXOS
DIVISION DE CONTRATOS

EL PRESENTE ANEXO CONSTA DE **57** HOJAS INCLUYENDO ESTA CARÁTULA

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

0070

FOLIO: 0000002733-2020

[ ] Dictamen de Inversión
[X] Dictamen de Gasto

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

Concepto: OFICIO NO. 1940 RECIBIDO EL 25/11/19 "SERVICIO DE SOPORTE TÉCNICO Y OPERACIÓN DE LA INFRAESTRUCTURA LÓGICA PARA LA MIGRACIÓN DE LA NUBE IMSS Y DRP 2020"

Fecha Elaboración: 25/11/2019

Total Comprometido (en pesos): $ 192,020,000.00
Cuenta: 42061506 SERV. INT. TEC DE INFO. Y COM.

Unidad de Información: 099001

Centro de Costos: 500000

ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
192,020.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
192,759.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

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

ATENTAMENTE

Lic. Jessica Miranda Vega

Titular de la División de Control y Seguimiento al Gasto de Operación

DIA MES AÑO
DICTAMINADO DEFINITIVO

DICTAMEN DEFINITIVO

CONTRATO No.

IMPORTE DEFINITIVO (EN PESOS): $ .00

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

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

Clave: 6170-009-001

ANEXOS
DIVISION DE CONTRATOS

SIN TEXTO

Contenido

ANEXOS
DIVISION DE CONTRATOS

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	27/09/2019	Elaboración de documento	Ing. Héctor Javier Reyes Oropeza Lic. Carlos Francisco Ramírez del Rivero Ing. Héctor Martínez Valenzuela Ing. Alejandro Paniagua Ramírez
0.2	30/09/2019	Actualización del documento	Ing. Javier Cortés López Ing. Carlos Calderón Zacarías
1.0	03/12/2019	Aprobación del documento	Ing. Eduardo Oropeza Ortiz

1. Objetivo del documento

Definir al LICITANTE los términos y condiciones del Servicio de Soporte Técnico y Operación de la Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube de IMSS y DRP.

2. Alcance del Servicio

Contar con el "Servicio de Soporte Técnico y Operación de la Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube de IMSS y DRP" cuyo fin es el de operar y soportar la infraestructura lógica mediante un modelo flexible y de consumo bajo demanda de los componentes tecnológicos de procesamiento, almacenamiento, virtualización, telecomunicaciones, seguridad, software (de administración, de virtualización, contenerización y monitoreo) orientando el servicio hacia un DRP.

El servicio mencionado previamente se podrá entregar para su consumo en:

- Centro de datos primario (CDP)
- Centros de datos alternos (CDA).
- Instalaciones designadas por el IMSS.

El servicio de soporte técnico y operación de la infraestructura lógica será consumido de la siguiente manera:

- Como "Nube Híbrida", que soportan los servicios digitales y de información, que requieren la interconexión con nubes públicas y privadas. Contará con la capacidad de intercambio de tráfico entre redes de telecomunicaciones, despliegue de canales digitales con reglas específicas de comunicaciones y seguridad, así como la capacidad de extensión de la nube híbrida en regiones geográficas estratégicas para mejorar la experiencia a usuarios externos en la entrega de servicios a través de una plataforma como servicio (PaaS). Haciendo énfasis en la integración con la Nube Privada, que se refieren a la capacidad de consumo tecnológico en las instalaciones designadas por el **IMSS**, con la finalidad de lograr algún nivel de integración, desde la capacidad de ser accedida a nivel de telecomunicaciones, hasta poder consumir o entregar información desde o hacia la Nube Privada.

El servicio será evaluado a través de acuerdos de Niveles de Servicio definidos en el presente documento, para mantener la operación de los servicios y soluciones, en apego a procesos determinados por la normatividad del IMSS, lo cual permitirá:

- Optimizar la atención de aprovisionamiento de infraestructura virtual bajo demanda.
- Mantener los niveles de operación y de seguridad requeridos por el **IMSS** en materia de TICs.
- Planear y probar el proceso de migración de la Nube de IMSS y DRP.
- Monitorear la disponibilidad de infraestructura virtual.
- Efectuar la gestión y resolución de incidentes en la operación de la infraestructura virtual.
- Ejecutar las actividades de aprovisionamiento y mantenimiento de infraestructura lógica.

3. Requerimientos Técnicos

El **LICITANTE** deberá realizar las actividades necesarias para la planeacion y pruebas de la migración y DRP, así como dar continuidad a la operación de los sistemas y aplicaciones Institucionales incluyendo la gestión y resolución de incidentes.

El **LICITANTE** deberá realizar las actividades correspondientes para soportar y operar la infraestructura lógica y virtual en el ámbito de la planeación y pruebas de la migración y DRP de conformidad a los niveles de servicio establecidos en el presente documento.

El servicio incluye lo siguiente:

- Servicios de operación
- Servicio de administración de proyectos
- Servicio de virtualización
- Servicio de respaldo y recuperación de información
- Servicio de operación en infraestructura de seguridad informática (ciberseguridad)
- Transferencia de conocimientos y adiestramiento tecnológico
- Repositorios de información
- CMBD de infraestructura tecnológica
- Soporte, operación y monitoreo de servicios digitales, así como sus componentes lógicos
- Proyección de un plan de migración
- Análisis de infraestructura, componentes, sistemas y servicios digitales para la continuidad de la operación, en casos de contingencia o desastre
- Creación y operación del plan DRP de los servicios.
- Soporte técnico para la plataforma de código abierto
- Operación de servicios de nube publica
- Soporte técnico y operación de la plataforma mainframe.

4. *Plazo de los servicios*

Los servicios tendrán vigencia a partir del 01 de enero y hasta el 29 de febrero de 2020..

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 para brindar el servicio **"Servicio de Soporte técnico y operación de la infraestructura lógica para la Migración de la Nube de IMSS y DRP 2020"** que permitan proveer al instituto las capacidades operativas para la Nube Hibrida IMSS, así como todo el soporte necesario para su funcionamiento, anexando un contrato de las mismas características o similiares al que se pretende contratar por parte del IMSS.

El **LICITANTE** deberá contar, con certificaciones en los rubros de procesamiento, comunicaciones, Gestion de Servicios de TI, Administración de Proyectos, Almacenamiento y seguridad tales como:

- **CCIE Routing and Switching**
- **CCIE Service Provider**
- **CCNP Colaboración**

- ☐CCDP Diseño Profesional de redes.
- ☐CCNA Cyber Ops
- ☐ITIL Foundation Certificate in IT Service Management
- ☐ITIL intermediate in Service Design
- ☐ITIL intermediate in Operational support and analysis
- ☐ITIL intermediate in Service Offering AND Agreements
- ☐ITIL intermediate un Release, control and validación.
- ☐Certificación ITIL RCV, 2017
- ☐Certificación ITIL SO, 2016
- ☐Certificación ITIL SOA, 2016
- ☐Certificación ITIL OSA, 2012
- ☐PMI
- ☐Symantec Data Loss Prevention Prevention 14.5
- ☐Symantec Messaging Gateway
- ☐APDS - Avaya Networking Solutions
- ☐APSS - Avaya Networking Solutions
- ☐ISO/IEC 27001
- ☐ISO/IEC 20000
- ☐PCNSE Network Security Engineer 7
- ☐MCITP Enterprise Administrator on Windows Server 2008
- ☐MCTS Microsoft Exchange Server 2007 Configuration
- ☐Extreme Networks Design Specialist - Campus Fabric
- ☐Enterasys Certified Specialist – Routing
- ☐Enterasys Certified Specialist – Policy.
- ☐Security Competency – Technical Accreditation (SCT)
- ☐Network Automation Competency – Technical Accreditation (NCT)
- ☐Core Network Services Competency - Technical Accreditation (CNT)
- ☐CCIE

El **LICITANTE** debe contar con el personal certificado en Metodologías de Administración de Proyectos para la dirección del proyecto emitido por el Project Manager Institute, cuando menos nivel PMP, presentando la certificación de cuando menos una persona que participará en la prestación del servicio.

El **LICITANTE** deberá presentar al Instituto, a través de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional cita en Av. Paseo de la Reforma No. 476, Anexo de Telecomunicaciones, Planta Alta, Col. Juárez, C.P. 06600, Ciudad de México, en un plazo no mayor a 5 (cinco) días naturales posteriores a la adjudicación del contrato, al personal responsable del proyecto; en caso que no se presente el personal en el plazo marcado, se aplicará la pena correspondiente.

El **LICITANTE** deberá presentar en un plazo no mayor a 10 (diez) días naturales posteriores a la adjudicación del contrato, un plan de trabajo general, para llevar a cabo la implementación del proyecto, en el que se especifiquen las actividades a realizar, la secuencia, los recursos asignados y responsables de dichas actividades, así como la duración del proyecto, su fecha de inicio y de conclusión marcando las fechas de entregables como son cantidad de servicios a entregar de forma única, mensual o eventual.

El **LICITANTE** deberá entregar en un plazo no mayor a 10 (diez) días naturales posteriores a la adjudicación del contrato, una matriz de escalación con el personal que gestionará los servicios de TIC y con los que el Instituto estará colaborando, su cargo y puesto así como los datos y la vía de comunicación para contactarlo.

ANEXOS
DIVISION DE CONTRATOS

6. Cumplimiento de obligaciones contractuales

Para la documentación de Cumplimiento de Obligaciones contractuales, el **LICITANTE** elaborará en un plazo no mayor a 10 (diez) días naturales posteriores a la adjudicación del contrato, una matriz de los verbos, pronombres, tiempos y compromisos presentes en el anexo técnico correspondiente, términos y condiciones, apéndices o documentación complementaria al anexo, así como en la propia oferta del **LICITANTE** ganador, a fin de contar con un listado de todos los verbos de acción, conjunciones, excepciones, interacciones, consideraciones de tipo y frecuencia de información electrónica que deba incluirse y en su caso especificaciones o excepciones, para convertirlos en los "documentos probatorios de cada obligación para la prestación del servicio".

A partir de este listado, de manera conjunta entre el **IMSS** y el **LICITANTE**, en un plazo no mayor a 05 (cinco) días naturales posteriores a la entrega del listado por parte del proveedor, generará el detalle de los documentos tanto en formato, contenido, información adjunta en imágenes, archivos o documentos complementarios, así como firmas y validaciones a efectuarse por el personal que participará en los procesos de entrega de servicios, lo cual se depositará en un repositorio documental que habilitará el **LICITANTE** con acceso permanente a los administradores del contrato (cuerpo de gobierno del contrato), los cuales analizarán al menos quincenalmente con el gerente de cuenta y personal técnico por parte del **LICITANTE**, el avance de los proyectos, la continuidad operativa, siguientes compromisos y la documentación del ejercicio del gasto y cumplimiento de niveles de servicio establecidos, siendo parte fundamental la documentación de Cumplimiento de Obligaciones contractuales, incluyendo en su caso, las deductivas aplicables. En estas juntas de gobierno del contrato, el **LICITANTE** deberá exponer al personal **IMSS**, los detalles de la operación, consumos, tendencias, áreas de oportunidad y mejores prácticas susceptibles de incorporarse a la operación y administración del contrato, las cuales serán evaluadas por el **IMSS** y en su caso, autorizadas con o sin modificaciones, para su implementación y operación gradual o inmediata.

Para la exposición y análisis de la información presentada por el **LICITANTE**, éste deberá habilitar al menos 3 pantallas de al menos 75 pulgadas, con todo lo necesario para la presentación de información de la operación de los servicios tecnológicos que permitan exponer de manera gráfica y ágil lo descrito en los dos párrafos anteriores, así como visualizar la información en línea de la operación de los servicios contratados incluyendo elementos de análisis y detalles de la operación (parámetros de utilización) de la infraestructura ofertada además de la prestación de los servicios, preferentemente reflejando la operación en términos de infraestructura además de indicadores de negocio que puedan ser descritos durante la vigencia del contrato.

7. Clausulas y Cumplimientos

a. Contrato de confidencialidad

El **LICITANTE** entregará al IMSS en un plazo no mayor a 05 días naturales al acto de fallo, una carta de confidencialidad mediante el cual el **LICITANTE** se obliga a no revelar, transferir, compartir ni ceder ningún dato o información de carácter sensible y confidencial que se hayan compartido entre el **LICITANTE** y el **IMSS**.

b. Cláusula de Opción para Obtención de Bienes al cierre de contrato (entregable de infraestructura)

El último mes de la prestación del servicio, el IMSS podrá evaluar quedarse con los bienes o conservar los bienes para lo cual informará al LICITANTE su decisión sobre la opción de compra de los bienes que integran el proyecto, el LICITANTE deberá presentar propuesta económica del o

los componentes de hardware/software que integran cada uno de los servicios descritos en el presente anexo técnico, así como sujetarse al procedimiento que establezca el IMSS para formalizar este proceso.

Durante el último mes de la prestación del servicio, en caso de que el Instituto haya optado por la opción de compra, el LICITANTE realizará el proceso de entrega del equipamiento sujeto a la opción de compra por parte del Instituto. El LICITANTE deberá sujetarse al procedimiento que el IMSS requiera para formalizar este proceso.

c. Documentación de cumplimiento de obligaciones

El **LICITANTE** con el objeto de fortalecer la supervisión y vigilancia de la administración del contrato materia del presente servicio y contribuir a las acciones para verificar la procedencia de los pagos, proporcionará un soporte especializado para la gestión del conocimiento administrativo relacionado con la prestación de los servicios de Nube **IMSS**.

Para que dicho conocimiento administrativo sea traducido en un activo del **IMSS**, el **LICITANTE** deberá aplicar el modelo de control de contratos definido por la Coordinación de Sistemas de Infraestructura Tecnológica Institucional (o la correspondiente por funciones organizacionales) y ejecutará las acciones que se establecen en dicho modelo como un ejercicio permanente durante la vigencia del contrato. Para tal efecto, se deberá implementar un mecanismo para que dicho soporte especializado encargado de la gestión del conocimiento administrativo de los servicios objeto del presente anexo, cuente oportunamente con cada una de las solicitudes de servicio que se generen en el marco del contrato respectivo, así como respecto de todos los comunicados y documentos existentes entre el **IMSS** y el **LICITANTE** en relación con la prestación de los servicios. Lo anterior, toda vez que los servicios de soporte especializados previstos en ese aparatado están sujetos a flujo de información antes citada.

Lo anterior, con el fin de que el **LICITANTE** elabore los "Reportes de Administración" con corte mensual, que concluya las acciones relacionadas a la facturación presentada durante el periodo de la prestación del servicio, cuyo contenido se señala a continuación:

Gestión de los servicios: Con base en las solicitudes u órdenes de servicio que genere el **IMSS**, el **LICITANTE** adjudicado incluirá un desglose detallado del trámite que corresponde a la atención de cada una de ellas, en cuanto a su procedencia, tiempos límite de respuestas y demás circunstancias que se encuentren establecidas en el contrato respectivo y que permitan al Administrador del mismo tener control sobre dicha gestión, así como la documentación probatoria del devengo de los servicios, incluyendo toda la documentación o archivos electrónicos que demuestren la prestación del servicio, de conformidad a la funcionalidad solicitada y acorde a los niveles de servicio establecidos, siendo posible entre otros: reportes de monitoreo, disponibilidad, capacidad, desempeño y atención de incidentes, tickets de la mesa, actualizaciones, bitácoras, logs de aplicaciones, entre otros. En caso de que el licitante no cuente con la documentación probatoria de los servicios devengados, estos no podrán ser facturados.

- **Plataforma de obligaciones:** En este apartado, el **LICITANTE** adjudicado elaborará un listado que identifique la totalidad de las obligaciones que se encuentran plasmadas en el contrato y sus respectivos anexos relacionados con los servicios. Asimismo, llevará a cabo su clasificación en atención a su importancia y consecuencia en:

  a. Obligaciones principales. Condicionantes del pago y los que están asociados a deductivas

ANEXOS
DIVISION DE CONTRATOS

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 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 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.

8. Administradores del contrato

El Instituto designará a los Administradores del Contrato, mismos que conforme a sus atribuciones serán los encargados de verificar que los servicios que administran se entreguen en los tiempos y las formas establecidos en el Anexo Técnico.

9. Derechos de Autor

El **LICITANTE adjudicado** deberá presentar escrito, a más tardar a los 05 (cinco) días naturales del acto de fallo, en el que se obliga a liberar al Instituto de toda responsabilidad de carácter civil, mercantil, penal o administrativa que, en su caso, se ocasione con motivo de la infracción de derechos de autor, patentes, marcas u otros derechos de propiedad industrial o intelectual a nivel nacional o internacional, además de no encontrarse en ninguno de los supuestos de infracción a la Ley Federal de Derechos de Autor, ni a la Ley de la Propiedad Industrial.

En el entendido de que en caso de que sobreviniera alguna reclamación en contra del Instituto, por cualquiera de las causas antes mencionada, el prestador del servicio se compromete a llevar a cabo las acciones necesarias para garantizar la liberación del Instituto de cualquier controversia o responsabilidad de carácter civil, mercantil, penal o administrativa, que en su caso, se ocasione.

10. Confidencialidad

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

De igual forma, será considerada como confidencial aquella información proporcionada por el Instituto para la ejecución del servicio que preste el **LICITANTE** adjudicado y sea propiedad exclusiva del Instituto.

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

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

ANEXOS
DIVISION DE CONTRATOS

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 el presente contratación, deberán entregar, de manera obligatoria, la Propuesta Técnica para realizar la respectiva evaluación de cada posible proveedor.

La Propuesta Técnica se presentará, tanto en formato impreso como en formato electrónico. En caso de que el Instituto detecte alguna diferencia entre la copia física y la electrónica, se considerará como elemento genuino el contenido del documento físico, siempre y cuando cumpla con los requisitos mencionados más adelante.

A continuación se puntualizan para su mejor atención los elementos, formatos y contenidos prioritarios para que la Propuesta Técnica pueda ser evaluada:

Presentación Física de la Propuesta Técnica

Los **LICITANTES** integrarán en su propuesta técnica algunos elementos, indispensables y con carácter de obligatorio, los cuales serán considerados por el Equipo Técnico designado por el Instituto durante la evaluación de las mismas. Las Propuestas Técnicas deben estar debidamente organizadas en carpetas, foliadas e incluirse un índice que indique clara y exactamente en dónde inicia y en dónde termina cada uno de los apartados y entregables correspondientes, para que el Equipo Técnico designado las revise ordenadamente. La propuesta técnica no es limitativa en alcance y extensión a los elementos aquí solicitados, sin embargo éstos son obligatorios de acuerdo a lo explicado en este documento.

Los participantes presentarán la propuesta técnica (en el caso de la impresa), debidamente organizada en las carpetas duras, separando las hojas en las carpetas por temas y/o capítulos, y también foliando las hojas de manera obligatoria desde la primera hasta la última en cada carpeta, para un mejor control del proceso de revisión técnica de las mismas. Cada carpeta debe contener tanto en su portada exterior, como en el lomo, un indicador que permita conocer el nombre del posible proveedor, el número de la carpeta, el identificador del proceso de contratación, y cualquier dato adicional que considere conveniente colocar y que apoye en la identificación del orden en que se integran. En la primera carpeta, además, el posible proveedor entregará un índice general de la información que entrega en cada carpeta, independientemente de los índices específicos de cada una de las carpetas.

Para el caso de la Propuesta Técnica electrónica, se solicita que dicha entrega se realice a través de medios ópticos (CD o DVD), o mediante dispositivos de almacenamiento tales como memorias tipo USB, todos estos deben estar debidamente protegidos mediante cajas de plástico o equivalentes, etiquetados e identificados con el nombre del **LICITANTE**, el número del medio óptico (en caso de ser más de uno), el identificador del procedimiento de contratación, y cualquier dato adicional que considere conveniente asentar de manera visible. El **LICITANTE** debe asegurarse de que el medio óptico pueda ser leído en lectores de disco convencional y que ha sido correctamente grabado. Puede incluir como respaldo, si así lo desea, módulos de memoria extraíbles o similares además del medio óptico.

El formato de archivos a almacenar de forma electrónica para la Propuesta Técnica, puede ser cualquiera de los siguientes:

- Microsoft Office Word
- Microsoft Office Excel
- Microsoft Office Poder Point
- PDF Postscript (Que permita la búsqueda de textos)
- Microsoft Office Visio
- Microsoft Office Project
- Formatos de imagen convencional (JPG, BMP, GIF, TIFF) para imágenes que no tengan una parte significativa de texto

Lenguaje

El **LICITANTE** será responsable de entregar su propuesta técnica preferentemente en lenguaje español. Sin embargo, dada la naturaleza del proyecto y de los servicios que se administrarán, se permitirá el uso de anglicismos generalmente aceptados en la industria, en aquellos términos que sean de origen extranjero, o que representen nombres de tecnologías particulares, sin embargo, incluirá el glosario de términos para su mejor comprensión.

En los casos donde así se indique, o que el **LICITANTE** juzgue necesario, será responsable de entregar documentación completa y detallada de los puntos en cuestión.

ANEXOS
DIVISION DE CONTRATOS

En los casos en los que esta documentación, sólo esté disponible en idioma inglés, se permitirá que el **LICITANTE** traduzca sólo el párrafo(s) que es de interés para el punto que se está documentando o citando, siempre y cuando el **LICITANTE** haga entrega del resto de la documentación en su formato e idioma original. Esta excepción sólo se hará para aquellos casos en donde la documentación requerida esté originalmente redactada en idioma inglés, y no se aceptarán propuestas que incluyan secciones de la documentación en ningún otro idioma que no sea inglés o español.

Diagramas

Todos los diagramas que formen parte de la propuesta técnica deben estar diseñados en Microsoft Visio o herramienta similar, y cada página estará debidamente rotulada, incluyendo el nombre del proyecto, el título del gráfico y el número de diagrama o figura.

Estos diagramas, junto con el resto de la presentación se entregarán en formato electrónico además del original en papel.

Información que debe contener la Propuesta Técnica

Los **LICITANTES** integrarán dentro de su propuesta técnica todos los entregables que a continuación se describen. Estos requisitos serán indispensables para verificar su capacidad operativa, tecnológica y técnica, para llevar a cabo satisfactoriamente la administración, operación, soporte e implementación de los servicios descritos en el Anexo Técnico correspondiente.

Los siguientes elementos son prioritarios e indispensables, por lo que se solicita a los participantes que en su propuesta incluya en carpetas, todos y cada uno de los entregables listados en la tabla siguiente, indicando correctamente la ubicación de cada uno de los siguientes rubros, para su fácil identificación y revisión, indicando el número identificador (ID) que aparece en la siguiente tabla:

No	Entregable
01	Aceptación de la totalidad de los capítulos y secciones contenidos en el Anexo Técnico correspondiente y Términos y Condiciones, para lo cual los participantes debe emplear el mismo orden y secuencia de temas que comprenden dichos documento, para manifestar su aceptación y compromiso explícito en todas y cada una de las solicitudes efectuadas como parte de los servicios, incorporando la glosa original del Anexo Técnico correspondiente para evitar ambigüedades en la suscripción.
02	Descripción a alto nivel de la arquitectura global que el **LICITANTE** utilizará para prestar los servicios objeto del Anexo Técnico correspondiente, apegándose a requerimientos del mismo. Este documento debe describir de forma general, las características de los componentes necesarios para entregar cada uno de los servicios, así como la estrategia que empleará para ajustarse al Plan General de Trabajo, pudiendo apoyarse para consolidar un documento concreto y conciso, en esquemas, diagramas, tablas, listados o cualquier elemento didáctico que el **LICITANTE** considere que aporta valor, para que el equipo técnico que el IMSS designe para la revisión de las propuestas, entienda los componentes, los servicios asociados, los procesos de servicio y sus características.
03	Manifestación escrita, firmada por el Representante Legal de la empresa participante, en la que establezca que cuenta con el soporte de los fabricantes de los Componentes Habilitadores de hardware y software ofertados, así como de los diferentes elementos de infraestructura auxiliar que incluya y que formen parte de la solución y; que cuenta con personal calificado para la prestación de los servicios ofertados.

No	Entregable
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

No aplica de conformidad con el Artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

13. Niveles de Servicio

El Servicio de Soporte Técnico y Operación de la Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube de IMSS y DRP se sujetará a los niveles de servicio establecidos en el apéndice respectivo del Anexo Técnico correspondiente.

14. Deductivas

- Los Administradores del Contrato serán los responsables de calcular y aplicar las 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.

ANEXOS
DIVISION DE CONTRATOS

15.Acuerdos de Niveles Operacionales

Con el objeto de garantizar la operación de los servicios, y de acuerdo con la metodología de administración de Niveles de Servicio ofertada, el **LICITANTE** adjudicado formalizará los Acuerdos de Nivel de Operación (OLA's) necesarios con el Instituto y con las entidades (terceros) involucradas en la provisión y uso de los servicios que demanda el presente proyecto, en coordinación con el Administrador del Contrato respectivo. Dichas entidades de terceros pueden entenderse también como otros proyectos o proveedores que fungen como componentes de la infraestructura habilitadora de los servicios objeto de este documento. Los OLAs se firmarán entre el Administrador del Contrato, en conjunto con el **LICITANTE** adjudicado y los demás administradores de contratos y/o servicios del Instituto con sus respectivos prestadores de servicios.

Los objetivos de los Acuerdos de Nivel de Operación son, de manera enunciativa más no limitativa, los siguientes:

- Definir y presentar los catálogos de servicio de distintos servicios, para identificar la participación de las diferentes áreas y prestadores de servicios de la organización para la entrega de los mismos.
- Delimitar las funciones del **LICITANTE** adjudicado y del personal que ejecuta los procesos de Negocio por parte del Instituto.
- Delimitar las funciones entre el **LICITANTE** adjudicado y otros prestadores de servicio que prestan servicios al Instituto, acordando un punto de demarcación definido por el alcance de los servicios señalados en el Anexo Técnico correspondiente; protegiendo ante cualquier circunstancia la continuidad de la operación del Instituto.
- Delimitar las funciones entre los prestadores de servicios actuales del Instituto que aún mantienen garantías vigentes de cualquier tipo de activo tecnológico en el alcance de este proyecto.

El **LICITANTE** adjudicado, entendido por el Instituto como un socio estratégico de su operación de TI y de los procesos de Negocio que son sustentados, así como los otros prestadores de servicios del Instituto, involucrados en dichos procesos de operación, trabajarán en conjunto para determinar los requerimientos y cumplir los compromisos que entre ellos se deriven a partir de los Acuerdos de Nivel de Operación.

16.Ubicaciones para la prestación del servicio

El LICITANTE adjudicado tiene la obligación de prestar sus servicios en la ubicaciones declararas en el presente documento o en las nuevas ubicaciones que el Instituto defina durante la vida del contrato resultante de este proceso, ya sea incrementando o sustituyendo alguna de las ubicaciones existentes, con objeto de acondicionar los servicios necesarios para su adecuado funcionamiento.

17.Consideraciones para la finalización del contrato

El LICITANTE adjudicado deberá tomar en cuenta, desde el arranque de la prestación de servicios, las medidas de previsión necesarias para cumplir con los requisitos señalados de manera referencial en éste apartado, verificados en la etapa final del servicio.

Durante el último mes de la vigencia 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.

18.Pago de los Servicios

El pago de los Servicios descritos en el Anexo Técnico correspondiente, serán de manera "Mensual" para los servicios recurrentes, por "Evento" para los que sean solicitados a discreción del Instituto y por "Única Ocasión", para los servicios que están planificados como única vez en la vida del contrato.

El LICITANTE adjudicado reportará y solicitará al Instituto el pago asociado a los servicios que haya entregado o que hayan sido consumidos, conforme a las especificaciones descritas en el Anexo Técnico correspondientes, con estricto apego a las características y niveles de servicio que se requieren para cada rubro definido en el catálogo de servicios, y que cumplan con los aspectos generales de su operación; sujeto a posibles deducciones por incumplimiento de los mismos, por lo que el Instituto, a través del Administrador del Contrato, evaluará y dictaminará las condiciones de funcionalidad, operatividad y consumo de los servicios que sean entregados por el LICITANTE adjudicado para que proceda el pago mensual que debe efectuarse por los mismos.

El LICITANTE adjudicado deberá presentar ante el respectivo Administrador del Contrato, la documentación comprobatoria (entregables) y Acta de Aceptación del Servicio, con la que acreditará fehacientemente que se ha proporcionado el servicio a entera satisfacción del Instituto, y en estricto apego al procedimiento administrativo vigente en el Instituto. Dichos servicios deberán sustentarse mediante la entrega documental al Instituto.

El LICITANTE adjudicado entregará oportunamente la factura por los servicios del mes, en la Coordinación de Servicios Administrativos de la Dirección de Innovación y Desarrollo Tecnológico, así como la nota de crédito respectiva, en caso de que aplique, para que sean debidamente sancionadas, de acuerdo con los requisitos fiscales que establece el artículo 29-A del Código Fiscal de la Federación.

El **LICITANTE** adjudicado expedirá sus facturas en el esquema de facturación electrónica CFDI (Comprobantes Fiscales Digitales por Internet). La recepción de las mismas será a través del Portal de Servicios a Proveedores, y deberán ser proporcionadas en su formato XML. La validez de las mismas será determinada durante la carga y únicamente las facturas físicamente válidas serán procedentes para pago. El **LICITANTE** adjudicado deberá proporcionar a los Administradores del Contrato una representación impresa de la misma que cumpla con las especificaciones normadas por el Servicio de Administración Tributaria (SAT). La representación impresa por sí misma no será sustento para pago si no se hace la carga del XML del cual se originó, o si la misma no es una representación fiel del XML origen.

Las facturas deberán reunir los requisitos fiscales establecidos en la Ley de la materia, indicando los servicios prestados, así como el número de contrato. Una vez validada la documentación anterior y previo cotejo con la coordinación responsable, se procederá a la liberación de la factura y documentación soporte del LICITANTE adjudicado, para que éste la entregue ante la División de Trámite de Erogaciones, en las oficinas que determine para tal efecto el Instituto.

En caso de que el LICITANTE adjudicado presente su factura con errores o deficiencias, conforme a lo previsto en el artículo 90 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el Instituto, dentro de los 3 (tres) días hábiles siguientes a la recepción, indicará por escrito al participante ganador las deficiencias que se deberán corregir.

ANEXOS
DIVISION DE CONTRATOS

El pago se realizará mediante transferencia electrónica de fondos, a través del esquema electrónico interbancario que el IMSS tiene en operación, a menos que el LICITANTE adjudicado en forma fehaciente la imposibilidad para ello.

El pago se depositará en la fecha programada de pago, si la cuenta bancaria del LICITANTE adjudicado está contratada con BANAMEX, HSBC, BANORTE, SANTANDER o SCOTIABANK, si la cuenta pertenece a un banco distinto a los mencionados, el IMSS realizará la instrucción de pago en la fecha programada, y su aplicación se llevará a cabo el día hábil siguiente, de acuerdo con lo establecido por el CECOBAN.

El pago se realizará en los plazos normados por la Dirección de Finanzas, en el "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago", sin que éstos rebasen los 20 (veinte) días naturales posteriores a aquel en que el prestador del servicio presente en la División de Trámite de Erogaciones del Instituto, ubicada en Gobernador Tiburcio Montiel Número 15, Colonia San Miguel Chapultepec, Código Postal 11850, Delegación Miguel Hidalgo, México Distrito Federal, en días y horas hábiles.

Las facturas que amparen los servicios cuya recepción no genere alta a través del SAI ni realice enlace al PREI de manera electrónica, deberán contener la firma de recepción y de autorización para el trámite de pago, de acuerdo a lo establecido en el Procedimiento para la recepción, glosa y aprobación de documentos para trámite de pago vigente.

En caso de que el **LICITANTE** adjudicado celebre contrato de cesión de derechos de cobro, deberá notificarlo por escrito al Instituto, con un mínimo de 05 (cinco) días naturales anteriores a la fecha de pago programado, entregando invariablemente una copia de los contra-recibos cuyo importe se cede. Además de los documentos sustantivos de dicha cesión, el mismo procedimiento aplicará en el caso de que el **LICITANTE** adjudicado celebre contrato de cesión de derechos de cobro a través de factoraje financiero conforme al Programa de Cadenas Productivas de Nacional Financiera, S.N.C., Institución de Banca de Desarrollo.

El pago de los servicios quedará condicionado proporcionalmente al pago que el **LICITANTE** adjudicado deba efectuar por concepto de deducciones.

Los impuestos y derechos que procedan con motivo de los servicios objeto de la presente adjudicación, serán pagados por el **LICITANTE** adjudicado, de conformidad a la legislación aplicable en la materia. El Instituto sólo cubrirá el impuesto al valor agregado (IVA) de acuerdo a lo establecido en las disposiciones legales vigentes en la materia.

El **LICITANTE** adjudicado deberá generar dichas facturas por períodos mensuales vencidos de servicio, y las entregará al Instituto en los primeros diez días naturales del mes siguiente al que se factura, de acuerdo con lo siguiente:

a) El **LICITANTE** adjudicado entregará la factura a la Coordinación de Servicios Administrativos de la DIDT.
b) La Coordinación de Servicios Administrativos enviará la factura a la Coordinación de Sistemas de Infraestructura Tecnológica Institucional para su trámite en términos del contrato.
c) La Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI) enviará al respectivo Administrador del contrato, la citada factura con la petición de que proceda a la validación de los servicios comprendidos en la misma, en su caso, emita la aceptación a entera satisfacción de los servicios.
d) Los Administradores del Contrato integrarán los respectivos sustentos documentales incluyendo los resultados del cálculo de las métricas de los niveles de servicio establecidos en el Anexo

Técnico para la aplicación de deducciones conducentes enviándola a la Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI).
e) La Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI) valida y enviará la documentación completa a la Coordinación de Servicios Administrativos para la gestión de pago.
f) La Coordinación de Servicios Administrativos entregará la factura al LICITANTE adjudicado.
g) El **LICITANTE** adjudicado deberá ingresar su factura y documentación al área de Trámite de Erogaciones para los trámites correspondientes.

19.Mecanismos de control para la administración del contrato

Rescisión administrativa del contrato.

En términos de lo dispuesto en el artículo 54, de la LAASSP, el Instituto podrá rescindir administrativamente el contrato en cualquier momento, cuando el **LICITANTE** adjudicado, incurra en incumplimiento de cualquiera de las obligaciones a su cargo, de conformidad con el procedimiento siguiente.

Si el Instituto considera que el **LICITANTE** adjudicado ha incurrido en alguna de las causales de rescisión que se consignan más adelante, lo hará saber al **LICITANTE** adjudicado, de forma indubitable por escrito, a efecto de que éste exponga lo que a su derecho convenga y aporte, en su caso, las pruebas que estime pertinentes, en un término de 5 (cinco) días hábiles, a partir de la notificación de la comunicación de referencia.

Transcurrido el término a que se refiere el párrafo anterior, el Instituto contará con un plazo de quince días para resolver, considerando los argumentos y pruebas que hubiere hecho valer el **LICITANTE** adjudicado. La determinación de dar o no por rescindido el contrato deberá ser debidamente fundada, motivada y comunicada al **LICITANTE** adjudicado dentro dicho plazo.

En caso de que el Instituto, determine dar por rescindido el contrato, se deberá formular y notificar un finiquito dentro de los 20 (veinte) días naturales siguientes a la fecha en que se notifique la rescisión, de conformidad con el artículo 99, del Reglamento de la LAASSP, en el que se hagan constar los pagos que, en su caso, deba efectuar el Instituto, por concepto del servicio, proporcionado por el **LICITANTE** adjudicado, hasta el momento en que se determine la rescisión administrativa.

En el supuesto de que se rescinda el contrato, el Instituto, no aplicará las penas correspondientes, 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 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

ANEXOS
DIVISION DE CONTRATOS

cumplir, a efecto de que el **LICITANTE** adjudicado, subsane el incumplimiento que hubiere motivado el inicio del procedimiento de rescisión. Lo anterior, se llevará a cabo a través de un convenio modificatorio en el que se atenderá a las condiciones previstas en los dos últimos párrafos del artículo 52, de la LAASSP.

Cuando por motivo del atraso en la entrega de los bienes o la prestación de los servicios, o el procedimiento de rescisión se ubique en un ejercicio fiscal diferente a aquél en que hubiere sido adjudicado el contrato, la dependencia o entidad convocante podrá recibir los bienes o servicios, previa verificación de que continúa vigente la necesidad de los mismos y se cuenta con partida y disponibilidad presupuestaria del ejercicio fiscal vigente, debiendo modificarse la vigencia del contrato con los precios originalmente pactados. Cualquier pacto en contrario a lo dispuesto en este artículo se considerará nulo.

El Instituto podrá rescindir administrativamente el contrato sin más responsabilidad para el mismo y sin necesidad de resolución judicial, cuando el **LICITANTE** adjudicado incurra en cualquiera de las causales siguientes.

1. Cuando no entregue la garantía de cumplimiento del contrato, dentro del término de diez días naturales posteriores a la firma del mismo.
2. Cuando incurra en falta de veracidad total o parcial respecto a la información proporcionada para la adjudicación o formalización del contrato.
3. Sea declarado en concurso mercantil o cualquier situación análoga o equivalente que afecte el patrimonio del **LICITANTE** adjudicado.
4. Cuando de manera reiterativa y constante, **LICITANTE** adjudicado sea sancionado por parte del IMSS con penalizaciones sobre el mismo concepto de los servicios prestados y con ello se afecten los intereses del IMSS.
5. Si la Comisión Federal de Competencia, de acuerdo a sus facultades, notifica al Instituto la sanción impuesta al **LICITANTE** adjudicado, con motivo de la colusión de precios en que hubiese incurrido durante el procedimiento, en contravención a lo dispuesto en los artículos 9, de la Ley Federal de Competencia Económica y 34, de la LAASSP.

Terminación anticipada del contrato.

En términos de lo establecido en el artículo 54 Bis, de la LAASSP, el Instituto podrá dar por terminado anticipadamente el contrato sin responsabilidad para éste y sin necesidad de que medie resolución judicial alguna, cuando concurran razones de interés general o bien, cuando por causas justificadas se extinga la necesidad de requerir los bienes o servicios objeto del presente contrato, y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas se ocasionaría algún daño o perjuicio al Instituto, o se determine la nulidad de los actos que dieron origen al contrato, con motivo de la resolución de una inconformidad o intervención de oficio emitida por la Secretaría de la Función Pública (SFP). En estos casos el Instituto reembolsará al **LICITANTE** adjudicado, los gastos no recuperables en que haya incurrido, siempre que éstos sean razonables, estén debidamente comprobados y se relacionen directamente con la contratación del servicio motivo del presente procedimiento de contratación.

20.Responsabilidad

El **LICITANTE** adjudicado se obliga a responder por su cuenta y riesgo de los daños que sean determinados por la autoridad judicial competente que por inobservancia o negligencia de su parte lleguen a causar al Instituto, con motivo de las obligaciones pactadas en este instrumento jurídico.

21.Responsabilidad Laboral

Queda expresamente estipulado que el personal para la prestación del servicio o que utilice el **LICITANTE** adjudicado para el cumplimiento de cualquiera de las obligaciones emanadas de este instrumento, estará bajo la responsabilidad única y directa de éste y por lo tanto, en ningún momento se considerará al Instituto como patrón sustituto o solidario, ni tampoco al **LICITANTE** adjudicado como intermediario, por lo que el Instituto no tendrá relación alguna de carácter laboral con dicho personal y consecuentemente queda liberado de cualquier responsabilidad laboral, fiscal, en materia de seguridad social, o de cualquier otra naturaleza jurídica, derivado de las disposiciones legales y demás ordenamientos en materia de trabajo y seguridad social, obligándose el **LICITANTE** adjudicado a responder de cualquier acción legal y/o reclamación que se pudiera presentar en contra del Instituto.

Independientemente de lo anterior, el **LICITANTE** adjudicado deberá de cumplir con las obligaciones en materia de seguridad social de sus trabajadores que van a prestar los servicios al Instituto, lo anterior en el marco de la Ley Federal del Trabajo vigente, en sus artículos 15-A, 15-B, 15-C y 15-D, por lo que "el Instituto" en cualquier momento podrá verificar su cumplimiento. Para lo cual el Instituto solicitará de manera mensual al proveedor el reporte mensual (Emisión IMSS).

22. Firmas de elaboración, revisión y aprobación

Responsables de Elaboración

Héctor Javier Reyes Oropeza
Titular de la División de Administración, Procesamiento y Almacenamiento
03/12/2019

Carlos Francisco Ramírez del Rivero,
Titular de la División de Administración y Continuidad de la Operación
03/12/2019

Héctor Martínez Valenzuela
Titular de la División de Telecomunicaciones
03/12/2019

Alejandro Paniagua Ramírez
Titular de la División de Administración de Riesgos Tecnológicos
03/12/2019

Responsables de Revisión

Javier Cortés López
Titular de la Coordinación Técnica de Operación de Servicios Tecnológicos
03/12/2019

Carlos Calderón Zacarías
Titular de la Coordinación Técnica de Redes y Telecomunicaciones
03/12/2019

ANEXOS
DIVISION DE CONTRATOS

Responsable de Aprobación

Eduardo Oropeza Ortiz
Titular de la Coordinación de
Sistemas de Infraestructura
Tecnológica Institucional
03/12/2019

INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

Anexo Técnico

Servicio de Soporte Técnico y Operación dela Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube de IMSS y DRP

Contenido

ANEXOS
DIVISION DE CONTRATOS

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	27/09/2019	Elaboración de documento	Ing. Héctor Javier Reyes Oropeza Lic. Carlos Francisco Ramírez del Rivero Ing. Héctor Martínez Valenzuela Ing. Alejandro Paniagua Ramírez
0.2	30/09/2019	Actualización del documento	Ing. Javier Cortés López Ing. Carlos Calderón Zacarías
1.0	03/12/2019	Aprobación del documento	Ing. Eduardo Oropeza Ortiz

1. OBJETIVO DEL DOCUMENTO

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

Clasificador Único de las Contrataciones Públicas (CUCOP): 31900002

2. OBJETIVO

El Instituto Mexicano del Seguro Social (IMSS) brinda servicios de seguridad social a más de 84 millones de derechohabientes, más de 3 millones de pensionados y cerca de 1 millón de patrones, a través múltiples aplicaciones, sistemas de información y servicios digitales ofrecidos en diversos canales de atención presenciales y no presenciales.

Para ello, el Instituto cuenta con 2 centros de datos propios el principal ubicado en la ciudad de Monterrey Nuevo León y el secundario en la Ciudad de México, así mismo cuenta con un contrato de centros de datos primario administrado por un tercero, denominado Servicios Administrados de Nube 2016-2019, que permite disponer de las capacidades de planeación, integración tecnológica, operación y seguridad enfocadas en habilitar el consumo como servicio de la infraestructura para el procesamiento, almacenamiento, comunicaciones, plataformas tecnológicas, y software.

Durante los últimos 6 años, el IMSS ha llevado a cabo una serie de acciones que van desde migrar sistemas legados de centros propios hacia el centro de datos administrado, así como el despliegue de servicios digitales y de información como parte de su evolución tecnológica y transformación digital, modernizando su plataforma web Institucional imss.gob.mx ofreciendo trámites y servicios no presenciales a la derechohabientes, trabajadores, patrones y ciudadanía en general.
Desde que el instituto inició su transformación digital en 2013 al mes de junio del 2019, se han obtenido los siguientes resultados:

- 656.4 millones de tramites digitales
- Recaudación de aproximadamente $1,400 millones de pesos diarios.
- Movimientos Afiliatorios de 986 mil patrones
- 51 millones de pagos referenciados
- 11 millones de citas médicas desde la app movil
- 9.1 millones de expedientes electrónicos
- 14.4 millones de recetas electrónicas expedidas
- 18.5 millones de constancias de semanas cotizadas
- 128.1 millones de avisos para control de servicios integrales
- 8.4 millones de cuentas por pagar

Si bien, la transformación digital del Instituto en los últimos años ha permitido mejorar los servicios ofrecidos hacia beneficiarios, trabajadores, patrones, ciudadanía y público en general, aún existen ecosistemas tecnológicos de gran impacto que requieren actualización diaria y complejos procesos manuales que implican un alto costo en la operación, que entre otras cosas soportan la recaudación de más de 1,400 millones de pesos diarios, el pago de nómina de más de 3 millones de pensionados, y el cálculo de la vigencia de derechos de más de 84 millones de derechohabientes.

La colaboración tecnológica entre los diferentes ecosistemas tanto propios como tercerizados, ha generado dependencias tecnológicas complejas en el intercambio de información para mantener la información coherente entre los diversos sistemas que involucran en las transacciones institucionales, tales como procesos relacionados a la Afiliación, Incorporación, Recaudación, Prestación Médica y Social, sin contar las nuevas arquitecturas propuestas basadas en esquemas de nube pública, privada e hibrida, y que transformará el modelo tecnológico y operativo del Instituto para tener mayor flexibilidad y esquemas de recuperación ante desastres, con esquemas automatizados y con menor dependencia humana.

Esto pone al instituto frente a un desafío tecnológico en un ecosistema diverso de sistemas, infraestructura, procesos de negocio e inclusive personal, que si bien es funcional, es necesaria una transformación hacia nuevos modelos operativos, tales como: Desarrollo de aplicaciones nativas de nube, elasticidad, resilencia y flexibilidad propios de una nube, así como modelos de operación automatizados, aprovisionamiento flexibles y bajo demanda, auto servicio, configuración automatizada de servicios, aplicaciones y componentes, respaldo y restauración de información y configuración de los sistemas y servicios, plataformas de virtualización basadas en contenedores, tropicalización de estándares definidos por el gobierno federal privilegiando el uso de plataformas abiertas, modelos de operación basados en estándares de la industria actual, así como esquemas de migración, y recuperación en caso de desastres entre los centros de datos del Instituto primordialmente de manera automática. Es por ello que el IMSS requiere contratar los servicios bajo demanda de soporte y operación de la infraestructura tecnológica de la nube IMSS acordes a su dinamica y necesidades operativas.

Para cumplir con lo anterior, y continuar con la mejora continua del servicio es necesario integrar nuevos esquemas de servicios que sean flexibles y que permitan el consumo tecnológico bajo demanda brindando una plataforma robusta que soporte, automatice y facilite la operación de los ambientes productivos, así como las plataformas que soportan los servicios digitales y de información que forman parte de la estrategia del Transfomación Digital IMSS. Lo anterior, permitirá proporcionar una mejor experiencia de usuario y al mismo tiempo fortalecer la experiencia de la interacción presencial dentro de las diferentes instalaciones del Instituto, con capacidad de crecimiento, innovación, evolución y mejora continua de todas sus plataformas.

3. ALCANCE

Contar con el "servicio de soporte técnico y operación de la infraestructura lógica" cuyo fin es el de operar y soportar la infraestructura lógica mediante un modelo flexible y de consumo bajo demanda de los componentes tecnológicos de procesamiento, almacenamiento, virtualización, telecomunicaciones, seguridad, software (de administración, de virtualización, contenerización y monitoreo) orientando el servicio hacia un DRP.

El servicio mencionado previamente se podrá entregar para su consumo en:

- Centro de datos primario (CDP)
- Centros de datos alternos (CDA).
- Instalaciones designadas por el IMSS.

El servicio de soporte técnico y operación de la infraestructura lógica será consumido de la siguiente manera:

- Como "Nube Híbrida", que soportan los servicios digitales y de información, que requieren la interconexión con nubes públicas y privadas. Contará con la capacidad de intercambio de tráfico entre redes de telecomunicaciones, despliegue de canales digitales con reglas específicas de

comunicaciones y seguridad, así como la capacidad de extensión de la nube híbrida en regiones geográficas estratégicas para mejorar la experiencia a usuarios externos en la entrega de servicios a través de una plataforma como servicio (PaaS). Haciendo énfasis en la integración con la Nube Privada, que se refieren a la capacidad de consumo tecnológico en las instalaciones designadas por el **IMSS**, con la finalidad de lograr algún nivel de integración, desde la capacidad de ser accedida a nivel de telecomunicaciones, hasta poder consumir o entregar información desde o hacia la Nube Privada.

El servicio será evaluado a través de acuerdos de Niveles de Servicio definidos en el presente documento, para mantener la operación de los servicios y soluciones, en apego a procesos determinados por la normatividad del IMSS, lo cual permitirá:

- Optimizar la atención de aprovisionamiento de infraestructura virtual bajo demanda.
- Mantener los niveles de operación y de seguridad requeridos por el **IMSS** en materia de TICs.
- Planear y probar el proceso de migración de la Nube de IMSS y DRP.
- Monitorear la disponibilidad de infraestructura virtual.
- Efectuar la gestión y resolución de incidentes en la operación de la infraestructura virtual.
- Ejecutar las actividades de aprovisionamiento y mantenimiento de infraestructura lógica.

4. REQUERIMIENTOS TÉCNICOS

El **LICITANTE** deberá realizar las actividades necesarias para la planeacion y pruebas de la migración y DRP, así como dar continuidad a la operación incluyendo la gestión y resolución de incidentes.

El **LICITANTE** deberá realizar las actividades correspondientes para soportar y operar la infraestructura lógica y virtual en el ambito de la planeación y pruebas de la migración y DRP de conformidad a los niveles de servicio establecidos en el presente documento.

El servicio incluye lo siguiente:

- Servicios de operación
- Servicio de administración de proyectos
- Servicio de virtualización
- Servicio de respaldo y recuperación de información
- Servicio de operación en infraestructura de seguridad informática (ciberseguridad)
- Transferencia de conocimientos y adiestramiento tecnológico
- Repositorios de información
- CMBD de infraestructura tecnológica
- Soporte, operación y monitoreo de servicios digitales, así como sus componentes lógicos
- Proyección de un plan de migración
- Análisis de infraestructura, componentes, sistemas y servicios digitales para la continuidad de la operación, en casos de contingencia o desastre
- Creación y operación del plan DRP de los servicios.
- Soporte técnico para la plataforma de código abierto
- Operación de servicios de nube publica
- Soporte técnico y operación de la plataforma mainframe.

Dichos alcances estarán en función de lo siguiente:

El aprovisionamiento bajo demanda de las Unidades de Servicio conforme los requerimientos del **IMSS**.

El aprovisionamiento bajo demanda de los Unidades de Servicio de Aprovisionamiento, partiendo de un ejercicio de planeación con el **IMSS** para determinar las diferentes plataformas que se requieren; y con base a ellas, establecer la definición y habilitación de las Unidades de Servicio de Aprovisionamiento a partir de las Unidades de Servicio.

Estas plataformas son de infraestructura virtualizada, así como de Extensión de Nube Privada y de aprovisionamiento de software como servicio: correo electrónico, colaboración, productividad personal y Escritorio en la nube.

Actividades relativas a la planeación y gobierno, actualización de la tecnología empleada en la nube y sus respectivos estándares y la integración de nuevas soluciones tecnológicas, canales y servicios a la nube.
Monitoreo y vigilancia del funcionamiento y desempeño de los Unidades de Servicio y Unidades de Servicio De Aprovisionamiento, así como de los servicios digitales y de información, y los sistemas informáticos y canales digitales que los soportan y se determinen por el **IMSS**.

La interconexión entre múltiples redes privadas de telecomunicación a través de un Punto Neutro de intercambio de tráfico, así como el despliegue de canales de acceso con otras nubes tanto públicas como privadas, en la que destaca el acceso a Internet y varias dependencias públicas.

El aprovisionamiento e instalación por cada nodo de extensión de la nube privada, configuración puesta en marcha, operación, mantenimiento, soporte y administración de Puntos de Acceso a la Nube Privada con capacidad de despliegue del servicio de Escritorio en la nube.

La provisión de servicios de administración y monitoreo relacionados a los Unidades de Servicio y Unidades de Servicio De Aprovisionamiento de la solución, tales como los de seguridad, optimización, Mesa de Ayuda, los servicios de Soporte Extendido y Documentación del Servicio a describir en las acciones específicas de este anexo.

Contar, de manera integrada y unificada, con los servicios administrados que permitan la continuidad operativa y de seguridad de la información de la Nube **IMSS** para ejecutar el plan de trabajo especificado.

Una vez iniciado los servicios el **LICITANTE** deberá dar cumplimiento al Plan de Trabajo detallado, cuya entrega será su responsabilidad, al amparo y cumplimiento del Plan de Trabajo General descrito en este documento, con el cual efectuará la migración sucesiva del universo de elementos dispuestos en el Servicio actual de Centro de Datos y Recuperación de desastres. Una vez que la migración se encuentre activa y operando a entrega satisfacción del Grupo Administrador del Contrato del **IMSS**, podrán ser incorporados al esquema de contraprestación de pagos mensuales.

En apego al mismo Plan de Trabajo General, donde el **LICITANTE** deberá presentar un programa anual para cada uno de los siguientes servicios:

- Arquitectura, gobierno y gestión del conocimiento.
- Centro de Operación de Seguridad
- Centro de continuidad a la operación
- Recuperación de desastres

Una vez aceptados dichos programas a entera satisfacción del Grupo de Administración del contrato, se comenzará a realizar las actividades de administración de cada servicio.

5. SERVICIOS DE OPERACIÓN

El objetivo del presente anexo técnico es establecer las especificaciones, calendarios, niveles de servicio, arquitecturas y lineamientos técnicos para la contratación de los servicios necesarios para la operación de la infraestructura lógica.

5.1 Gestión y resolución de incidentes, asi como atención de solicitudes relacionadas a la infraestructura virtual.

El **LICITANTE** deberá implementar un punto único de contacto para recibir, registrar, categorizar, dar seguimiento y generar información de los procesos de Gestión de Requerimientos, Gestión y resolución de Incidentes, Gestión de Cambios y Gestión de Problemas, relacionados a los servicios de infraestructura virtual y apegado a los procesos ITIL para la atención de problemas, incidentes y solicitudes con una cobertura de 7x24x365. A continuación, se describen de manera enunciativa más no limitativa, algunos de los eventos que se podrán reportar en la Mesa de Servicio:

- Falla en componentes virtuales
- Degradación del desempeño en las aplicaciones, componentes o servicios virtuales
- Fallas y/o degradación de funcionamiento en Sistema Operativo, Bases de Datos, comunicaciones o cualquier componente virtual
- Cualquier falla o degradación que se detecte en los servicios o la infraestructura lógica relacionados con el servicio de migración o DRP

A fin de que el registro de un ticket, categorización y asignación se realice en el menor tiempo posible y se proporcione la información necesaria suficiente para su atención, el **LICITANTE** deberá realizar las acciones, en conjunto con el **IMSS**, para que cuente con la siguiente información que deberá configurar en la solución tecnológica:

- Guion de atención y catálogo de servicios.
- Matriz de escalamiento.
- Guiones de atención al primer nivel de soporte y/o recabar la información requerida por los grupos de soporte para la atención del ticket.
- Categorizaciones de casos
- Grupos de soporte

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

El **LICITANTE** deberá proporcionar los mecanismos necesarios para realizar la integración necesaria con de la mesa de servicios ofertada hacia la mesa de servicios Institucional.

Las herramientas, soporte tecnico, personal, infraestructura y proceso de atención de la Mesa de Servicio ofertada al IMSS deberán estar personalizados para la atención al **IMSS,** garantizando la continuidad, seguridad y confidencialidad.

El proceso de atención de la Mesa de Servicio deberá ser propuesto por el LICITANTE y en su caso, adecuado y o autorizado por el IMSS.

Los tickets generados por la Mesa de Servicio deberán ser despachados hacia grupos de soporte establecidos por categorización acorde a lo definido entre el Instituto y el LICITANTE, cuidando en todo momento lo siguiente:

- El LICITANTE deberá contar con una herramienta automatizada para la detección de incidentes o eventos, su registro, notificación, administración, seguimiento y todo lo necesario hasta su resolución, incluyendo mecanismos electrónicos para el seguimiento del avance en la resolución del incidente.
- La Mesa de Servicio debe despachar inmediatamente el ticket con los grupos de soporte definidos para la atención del evento reportado.
- Todos los tickets deberán registrar el horario en que sean creados para el seguimiento de atención y servicio.
- Los tickets deberán ser cerrados hasta que el incidente o el evento que lo generó haya sido solucionado por completo y confirmado por parte del Instituto, por cualquiera de los canales que habilite la mesa, siempre y cuando se genere evidencia de la confirmación del usuario.

Los tiempos de atención y solución proporcionados por el **LICITANTE**, tanto para solicitudes como para incidentes o problemas deberán ser validados y autorizados por el **IMSS** en las mesas de trabajo al inicio del contrato.

5.2 Productos

Durante los 10 días naturales al mes vencido, el **LICITANTE** deberá enviar al **IMSS** el reporte impreso y firmado por el apoderado legal del licitante, referente a los tickets generados en el mes vencido. Dicho reporte deberá tener al menos los siguientes campos:

- Numero de ticket.
- Fecha y hora de creación.
- Descripción de lo reportado.
- Nombre o nombres del personal que atendieron el ticket.
- Descripción de la solución y en su caso, reporte postmortem.
- Fecha y hora de la solución.
- Fecha y hora el cierre.
- Tiempo de atención del incidente, requerimiento o ticket.
- Nivel de servicio definido para este tipo de incidente.
- Tiempos acumulados de afectación para este tipo de incidente en el mes en curso.
- En su caso, posible deductiva correspondiente.

5.3 Entrega y operación de servicios

El **IMSS** requiere contar con el servicio de mantenimiento preventivo y/o correctivo para todas las plataformas tecnológicas virtuales que forman parte del Servicio.

El **LICITANTE** debe contar con un Centro de Atención permanente durante las 24 horas del día y durante la vigencia del contrato, debiendo proporcionar el soporte técnico que corresponda al horario y vigencia de la contratación del servicio, a través del cual el **IMSS** pueda levantar reportes para solicitar soporte y asesoría técnica telefonica (ilimitada e inmediata).

El **LICITANTE** debe brindar un tiempo de respuesta inmediato catalogando por grado de severidad de la contingencia presentada, comprometiéndose a un tiempo máximo de resolución indicando en los niveles de servicio; asimismo el **IMSS** podrá solicitar al **LICITANTE** que el servicio se realice en el horario más conveniente para la Organización.

En caso de que el **LICITANTE** del servicio no pueda resolver el problema y se requiera el apoyo directo del fabricante, el **IMSS** deberá tener acceso por medio del **LICITANTE** a los servicios de soporte y atención del fabricante, así como acceso a su centro de atención.

Los **LICITANTES** deberán considerar en sus propuestas técnica y económica, la asignación de los recursos técnicos, humanos y de infraestructura necesarios para resolver, a partir del inicio del contrato toda solicitud referente a este punto y deberá prestarse a todas las plataformas tecnológicas virtuales que forman parte del servicio.

Los Mantenimientos preventivos y/o correctivos a la infraestructura virtual deberán ser supervisados por los recursos provistos por el **LICITANTE**.

El servicio de mantenimiento preventivos y/o correctivos consistirán de manera enunciativa, más no limitativa, de las siguientes actividades:

- Reparación, reinstalación y/o reemplazo de la infraestructura virtual.
- Instalación y/o reinstalación de software institucional y de parches, fixes, actualización, incorporación al directorio activo, entre otros.
- Restauración de configuraciones y parámetros.
- Elaboración de análisis, estudios, diagnósticos y pruebas para la detección de causales que tengan como consecuencia un mal funcionamiento de los equipos físicos y lógicos considerados en este contrato, siendo obligación del **LICITANTE** la entrega de alternativas de solución.

El mantenimiento preventivos y/o correctivos se realizará cuantas veces sea necesario en función a las eventualidades o fallas que se presenten durante la vigencia del contrato.

5.4 Servicios de mantenimiento preventivos y/o correctivos

El **LICITANTE** deberá considerar los mantenimientos preventivos y/o correctivos necesarios en caso de falla de alguna de los elementos de infraestructura lógica en los tiempos de atención y niveles de servicio solicitados.

El **LICITANTE** deberá reconfigurar, instalar o en su defecto reemplazar los componentes de infraestructura lógica dañados y restablecer los servicios operativos de acuerdo a la criticidad, el cual se detalla la sección de "Administración del Nivel de Servicio".

La infraestructura lógica que el **LICITANTE** reconfigure o instale deberán ser de las mismas características que el activo degradado o dañado.

En el caso de los mantenimientos preventivos y/o correctivos deberán cumplir con lo siguiente:

- Durante las actividades de mantenimiento preventivos y/o correctivos el **LICITANTE** deberá llevar a cabo rutinas de diagnóstico del buen funcionamiento de la infraestructura lógica, a fin de garantizar el

correcto funcionamiento de todos los equipos. En caso de identificar alguna anomalía con alguno de los equipos, emitirá recomendaciones al **IMSS** para corregir la falla, previo visto bueno del **IMSS**.

- El **LICITANTE** del servicio deberá llevar a cabo el diagnóstico para garantizar el correcto funcionamiento de todas las tarjetas, interfaces, cables y demás aditamentos que conforman la base de infraestructura lógica, asimismo en caso de existir deberá localizar y corregir las fallas.
- Dentro del programa de operación, será necesario realizar las actividades inherentes a los respaldos de configuración de todos los equipos. Dichos respaldos deberán ser entregados para su resguardo al personal que designe el **IMSS**.
- El **LICITANTE** deberá definir en conjunto con el **IMSS** las ventanas de mantenimiento para la realización de las actividades de mantenimiento correctivo, mediante un plan de trabajo y documentarlo a través de un control de cambios (RFC "Request for Change").

El **LICITANTE** deberá optimizar los recursos y configuraciones de la red y de seguridad, previa instalación de las configuraciones de infraestructura lógica que suministre. Asimismo, deberá tomar las debidas precauciones para evitar interrupciones en el servicio en la etapa de planeación y pruebas de la migración e instalación de la infraestructura lógica y DRP.

5.5 Procedimiento para reporte de fallas

El licitante deberá contar con una herramienta electrónica para la detección automatizada de incidentes o eventos en la infraestructura virtual, debiendo generar de manera automática registro en la herramienta de mesa de servicio, así como los alertamientos al personal del IMSS establecidos en las mesas de trabajo al inicio del contrato.

El reporte de fallas podrá ser en cualquier horario (7X24X365 durante la vigencia del contrato). El tiempo estipulado para restituir el servicio dependerá del tipo de falla que se presente, el tiempo de resolución de falla se indica en el apartado de Niveles de Servicio.

El **LICITANTE** deberá considerar para la implementación de la infraestructura lógica, incluyendo como mínimo las siguientes actividades:

- Plan de implementación de la infraestructura lógica.
- Instalación de los equipos.
- Interconexión de la infraestructura lógica.
- Configuración tipo de la infraestructura.
- Configuración de protocolos.
- Configuración de ruteo.
- Configuración de reglas.
- Configuración de QoS.
- Configuración de multicast en la red para transmitir señales de voz, datos y video.
- Migración de configuraciones de la infraestructura lógica anterior a la infraestructura lógica nueva.
- Configuración de parámetros básicos para monitoreo y administración.
- Configuración para protección de ataques conocidos.
- Configuración de alta disponibilidad.
- Configuración de temas de seguridad lógica.
- Configuración y puesta a punto de los activos tecnológicos lógicos.
- Aplicación de las mejores prácticas de la industria en las materias de infraestructuras tecnologicas virtuales en comento.
- Migración de infraestructura lógica.

Y todas aquellas tareas o configuraciones necesarias en la implementación que el **IMSS** considere necesarias para su correcta operación.

5.6 Administración de soporte remoto

Con la finalidad de proporcionar soporte técnico a las diversas infraestructuras tecnológicas del **IMSS**, el **LICITANTE** deberá considerar que podrá hacer uso de herramientas de soporte remoto, la cual permita gestionar apoyo de otros ingenieros a distancia para que los incidentes presentados puedan ser resueltos de manera inmediata en sitio o donde sea necesaria la intervención de especialistas de soporte de nivel superior. En caso de que el apoyo remoto sea necesario, este deberá ser aprobado de manera previa por el IMSS mediante los mecanismos electrónicos que proponga el licitante y sean autorizados por el Instituto en las mesas de trabajo al inicio del contrato.

5.7 Políticas y procedimientos

En coordinación el **LICITANTE** y el **IMSS**, definirán los procesos y procedimientos relacionados a la atención de llamadas, escalamiento y todos aquellos procesos que definan la operatividad interna del servicio, alineándose a la normatividad que le aplique (MAAGTICSI o la normatividad aplicable vigente). Una vez definidos será responsabilidad del **LICITANTE** el implementarlos y ejecutarlos durante toda la duración del contrato.

6 SERVICIO DE VIRTUALIZACIÓN

El **LICITANTE** entregará mediante los mecanismos de administración del servicio las herramientas para la ejecución del soporte a nivel de los servicios virtuales y sus componentes, dándole un seguimiento mediante los mecanismos propiamente mencionados para la correcta administración del servicio mencionado.

El **LICITANTE** entregará una plataforma de virtualización de plataforma abierta, tipo RHEV o equivalente que incluya suscripción de soporte técnico empresarial, que permita al **IMSS** desarrollar plenamente las actividades del servicio.

6.1 Unidad Integral de Virtualización Red Hat o compatible.

El **LICITANTE** entregará mediante los mecanismos, las herramientas, servicios virtuales y sus componentes, entregando una plataforma de virtualización RHEV o compatible, que permita al IMSS desarrollar plenamente el despliegue de los componentes virtuales que integran esta solución, lo anterior deberá incluir al menos lo siguiente:

- Red Hat Enterprise Linux Smart Virtualization o compatible.
- Red Hat OpenShift Container Platform Standard, 2-Core o compatible.
- Red Hat Ansible Automation Standard (100 Managed Nodes) o compatible
- Red Hat CloudForms Premium (Managed Nodes: Physical (2 sockets) or Virtual (16), public cloud) o compatible.

La unidad integral de virtualización deberá tener soporte durante la vigencia del contrato y la cual deberá incluir todos los componentes necesarios para su correcto funcionamiento.

Adicionalmente, el proveedor deberá incluir dentro de su propuesta la instalación del software Red Hat Enterprise Linux por nodo solicitado por el IMSS o compatible. Así mismo, el proveedor deberá incluir la instalación de las plataformas Red Hat OpenShift Container, Red Hat Ansible Automation y Red Hat

CloudForms o software compatible. Lo anterior, deberá estar funcionando de forma correcta y deberá contemplar todos los componentes necesarios para su operación sin costo adicional para el Instituto.

6.2 Operación de Infraestructura de Virtualización

El **LICITANTE** deberá suministrar el servicio de soporte técnico empresarial sobre la plataforma de virtualización abierta, la cual deberá ser RedHat RHEV o equivalente, donde acotara las soluciones de software, el hardware, y los componentes involucrados en el diseño o arquitectura.

El **LICITANTE** deberá suministrar el servicio de soporte técnico empresarial sobre la plataforma de virtualización ofertada, el cual se acotará a las soluciones de software, el hardware, y los componentes involucrados en el diseño o arquitectura.

El **LICITANTE** entregará el servicio de operación contemplando la ejecución, administración de las plataformas, para su óptimo funcionamiento.

El **LICITANTE** debe brindar el soporte en creación y administración de máquinas virtuales, y asegurar el correcto despliegue de las mismas, brindando apoyo en el seguimiento y entrega de requerimientos del **IMSS**. El **LICITANTE** entregará el servicio de los sistemas operativos (huéspedes) que se ejecutan sobre el entorno virtual (VMs) en base a lo establecido por el **IMSS**, respetando versiones de SO y parches solicitados.

El **LICITANTE** brindará el soporte técnico empresarial que involucre reconfigurar o extender recursos sobre la 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.

El **LICITANTE** efectuará las actividades del equipo técnico a su cargo, para efectuar labores sobre la solución de virtualización a efecto del permitir el mantenimiento a los equipos físicos en colaboración con los distintos equipos de trabajo involucrados, la acción de migrar servicios de manera automatizada y transparente sobre la plataforma de virtualización, representando un movimiento de las máquinas virtuales, almacenamiento o contenedores a otras plataformas activas.

El **LICITANTE** deberá supervisar y garantizar que la plataforma de virtualización mantendrá un balanceo dinámico de los recursos de hardware asignados a una o más de las máquinas virtuales del **IMSS**. Lo que representa una relocalización de máquinas virtuales, almacenamiento o contenedores en componentes de la plataforma con menor carga de trabajo en recursos.

El **LICITANTE** brindará soporte proactivo sobre la plataforma de virtualización para prevenir interrupciones, en el servicio a causa de fallas, proporcionando un ambiente de alta disponibilidad en servicios o procesos las máquinas virtuales del **IMSS** con una o más plataformas de virtualización activas.

El soporte brindado sobre la plataforma de virtualización se llevará a cabo empleando preferentemente métodos automatizados a través de scripts para la orquestación de la configuración, o en su defecto, si es justificado, utilizando mecanismos centralizados.

El **LICITANTE** deberá proporcionar un repositorio en el que se almacene todos los scripts de configuración de los servicios virtualizados ordenados por funcionalidad y siguiendo las mejores prácticas de la tecnología implementada.

El LICITANTE deberá ejecutar las acciones de respaldo de la información contenida en las máquinas virtuales, contenedores o cualquier otro elemento virtualizado, acorde a las políticas de respaldo del Instituto.

6.3 Aplicación de ajustes de operación sobre la infraestructura virtual

El **LICITANTE** deberá ejecutar durante la vida del contrato, de manera pro-activa y periódica, las siguientes actividades: identificación, análisis, propuesta y ejecución (previa autorización del Instituto) de optimización de la plataforma de virtualización y su contenido, aplicando las configuraciones necesarias que aporten al cumplimiento y/o mejora de los niveles de servicio establecidos en el presente documento y para la ejecución de las pruebas de migración. Deberá a su vez entregar el reporte con las actividades inherentes a las tareas descritas así como el impacto cualitativo y cuantitativo de las optimizaciones.

6.4 Configuración de Redes y Telecomunicaciones Virtuales

El **LICITANTE** deberá cumplir con la puesta e instalación de la conectividad en red dentro del entorno de virtualización y fuera del mismo, utilizando protocolos y mejores prácticas de la industria que generen esquemas para mantener los niveles de servicio establecidos en el presente documento, relacionadas a las pruebas de migración establecidas por el Instituto.

La plataforma de virtualización que será operada por el **LICITANTE** deberá tener la capacidad de aprovisionar los servicios de red de manera dinámica, definiendo el uso compartido de los recursos de red y utilizando switches distribuidos, los cuales existirán como elemento fundamental de la red en cada servidor físico (nodo) del ambiente virtual, formado por grupos o clústers, administrados preferentemente por métodos automatizados a través de scripts para la orquestación de la configuración, o en su defecto, si es justificado, utilizando mecanismos centralizados. Los Switches físicos y virtuales deberán soportar y ser compatibles con:

- Soporte de VLANs privadas
- Soporte de reenvió/transporte de tráfico en capa 2 (del modelo OSI)
- Soporte de enlaces troncales con etiquetado de VLANs (IEEE 802.1Q)
- Soporte de segmentación en capa 2 (VLAN segmentación)

6.5 Actualización y Mantenimiento de Infraestructura Virtual

El **LICITANTE** será responsable de designar encargados de la gestión y seguimiento del procedimiento preventivo, actualizaciones y correcciones. Para realizar de manera coordinada con el Instituto las actividades de mantenimiento presentando el respectivo plan de trabajo con la propuesta de calendarización.

Los mantenimientos no deberán interrumpir la continuidad operativa de los servicios Institucionales y las pruebas de migración, en cuyo caso la falta de continuidad operativa, será sujeta a las deductivas correspondientes. Para garantizar lo anterior, se evaluará la ejecución de actividades del plan de trabajo en el tiempo establecido y de presentarse algún retraso, se evaluará contra niveles de servicio; mismo caso para los eventos en los que por la aplicación del mantenimiento en tiempo establecido en el plan de trabajo, se dé una baja de la continuidad.

Los mantenimientos y actualizaciones se realizarán de acuerdo con los siguientes puntos:

- Políticas y procedimientos documentados

El **LICITANTE** desarrollará las políticas y procedimientos para la ejecución de las siguientes actividades: reinicio de componentes, depuración de logs, instalación de parches y/o hotfixes, depuración de almacenamiento, actualizaciones tecnológicas, entre otras que puedan ser relacionados al servicio de virtualización.

- Calendario de ejecución

El **LICITANTE** será responsable de proponer y acordar con las áreas que sean correspondientes en el **IMSS**, las fechas para la ejecución de los mantenimientos preventivos en la plataforma virtual de los ambientes involucrados con la finalidad de tener el menor impacto a la operación de los sistemas y aplicativos.

- Desarrollo de ejecución y plan de trabajo

El **LICITANTE** será responsable de coordinar e integrar con los terceros involucrados, el plan de trabajo del mantenimiento de la plataforma de virtualización y su contenido, el cual deberá ser aplicado por el **LICITANTE** en las plataformas virtuales.

- Investigación y recomendaciones

El **LICITANTE** será responsable de identificar, relacionar y elaborar una propuesta para la instalación de parches y/o hotfixes que permita llevarlos al último nivel de actualización estable (recomendado por el fabricante) y/o documentar las excepciones correspondientes, considerando la mitigación de posibles impactos y configuraciones certificadas por el fabricante o un tercero que se encuentre certificado.

- Acceso y descarga de insumos

El **LICITANTE** será responsable de implementar los mecanismos necesarios y suficientes para garantizar el acceso al personal del IMSS y del LICITANTE, a las plataformas del fabricante y bases de conocimientos, para revisar y descargar documentación y medias de instalación propias del proceso de actualización, que compongan la plataforma de virtualización.

Previo a la actualización de los componentes de las plataformas de virtualización, el **LICITANTE** deberá efectuar los respaldos correspondientes con la finalidad de poder garantizar un punto de retorno en caso de presentar alguna desviación en el proceso de actualización.

- Registro de parches e ingreso al Proceso de Liberaciones y/o Cambios

El **LICITANTE** realizará y sustentará un dictamen técnico para determinar la prioridad de implementación de los parches en los ambientes soportados, agrupando de acuerdo a prioridades (URGENTE, ALTA, MEDIA, y BAJA). Con base en dicha prioridad, deberá coordinar y desarrollar las actividades necesarias para integrarlas al plan de trabajo de actualización de parches y/o hotfixies e iniciar la gestión para su ingreso.

6.6 Gestión de Incidentes de la Infraestructura Virtual (Lógica)

Se considerará un incidente a una interrupción no planificada o reducción en la calidad de servicio de la Nube **IMSS**. También será considerado un incidente a la falla de un elemento de configuración de la plataforma de virtualización. Será considerado un incidente mayor aquel que deja fuera de operación al menos un servicio crítico del **IMSS**. Se deberá establecer, en conjunto con el **IMSS**, un procedimiento especial para la atención de incidentes mayores.

El proceso administrado por el licitante, deberá restablecer la operación del servicio acorde en los niveles de servicio establecidos en el presente documento, minimizando el impacto en las pruebas para la migración **IMSS**.

Para la gestión de incidentes, el **LICITANTE** deberá contar con equipos de trabajo (personal) especializados en la gestión y deberán, coordinarse con los grupos de soporte y gestión del **IMSS** o quien este señale. El grupo de gestión de incidentes del LICITANTE deberá tener al menos un coordinador de incidentes (propuesto por el LICITANTE y autorizado por el INSTITUTO) disponible en un esquema de atención 7x24. De igual forma, deberá tener grupos de soporte establecidos de acuerdo a lo siguiente:

- Primer nivel de atención: Especialistas en desarrollo de software.
- Segundo nivel de atención: Especialistas en la plataforma de virtualización y el ecosistema operativo.
- Tercer nivel de atención: Especialistas del fabricante (hardware y/o software).

El **LICITANTE** deberá cumplir con los niveles de escalamiento que se definan en conjunto con el **IMSS**. Estos niveles de escalamiento deberán establecerse durante las mesas de planeación del arranque. Así mismo, deberá establecer un procedimiento específico para la atención de incidentes mayores que define tiempos menores de escalamiento y criterio para establecer la prioridad al nivel que otorgue atención en el menor tiempo sobre el resto de los incidentes.

El **LICITANTE** deberá habilitar, actualizar y depurar los foros sociales por distintos canales para el seguimiento de incidentes, siendo responsabilidad del proveedor la posible fuga de información por omisión de las actividades de depuración y actualización, o en su caso la falta de distribución al personal procedente. Estos foros deberán estar coordinados por el Coordinador de Incidentes del LICITANTE y deberán integrar a las personas que el **IMSS** determine para la resolución de cada incidente.

El **LICITANTE** deberá entregar, en un plazo no mayor a 24 horas posterior a la solución del incidente, un reporte de análisis "post-mortem" de los incidentes mayores, o aquellos que el **IMSS** solicite. El contenido del reporte será especificado durante las mesas de planeación del arranque.

Actividades a cargo de los grupos de soporte del **LICITANTE**

- Operar la plataforma de virtualización a fin de garantizar la continuidad operativa.
- Efectuar la gestión de incidentes hasta su solución acorde a:
  - Identificar y registrar los incidentes
  - Categorizar, priorizar y realizar diagnóstico inicial
  - Investigar y diagnosticar
  - Solucionar y recuperar
  - Cerrar el incidente
- Informar al **IMSS** el estado de los incidentes
- Generar el reporte "post-mortem" (en caso de aplicar)

Actividades del Coordinador de incidentes del **LICITANTE**

- Organizar, conformar y coordinar los grupos de soporte del primero, segundo y tercer nivel.
- Gestionar la atención de los incidentes.
- Ser el enlace con el **IMSS** para dar información y seguimiento de los incidentes.
- Monitorear la efectividad del proceso de la gestión de incidentes e implementar acciones de mejora al proceso, previa autorización por el INSTITUTO.
- Escalar al siguiente nivel de atención en caso necesario.

- Administrar los foros sociales acorde a lo descrito anteriormente.
- Recopilación de los insumos necesarios para la solución del Incidente tales como:
  - Reportes de las herramientas de monitoreo
  - Bitácoras de la infraestructura virtual (Logs)
  - Evidencia del incidente
  - Base de conocimiento de errores conocidos
  - CMDB
  - Repositorio de arquitectura
  - Información y evidencia de las acciones realizadas en los componentes y servicios relacionados con el incidente
  - Información y evidencia de la solución de incidentes ocurridos previamente
  - Productos durante el incidente
  - Registro de incidentes en la solución tecnológica para análisis de problemas
  - Reporte semanal de incidentes
  - Informe "post-mortem"
  - Reporte de cambios realizados para soluciones incidentes.

6.7 Monitoreo y reportes de Infraestructura Virtual

El **LICITANTE** deberá brindar y cumplir con Instalación y puesta a punto de un sistema de monitoreo para dar visibilidad de los indicadores de desempeño y salud de la infraestructura virtual, que permita alertar de manera proactiva y disparar acciones preventivas, correctivas y de continuidad en el servicio, agrupando para su despliegue la infraestructura en términos de su uso por dirección normativa e indicadores de negocio.
El **LICITANTE** ejecutará las tareas de monitoreo mediante herramientas propias o de terceros de las plataformas de virtualización o software dedicado para análisis de datos.

El **LICITANTE** mediante las acciones de monitoreo buscará ejecutar acciones proactivas necesarias para detectar desviaciones en los umbrales establecidos para dar continuidad de la operación así como mostrar los indicadores de negocio, que se definirán de manera conjunta con personal del Instituto y proveedores externos.

El **LICITANTE** deberá configurar cualquier integración con herramientas de monitoreo del Instituto, o bien brindar cualquier elemento (Servicio web, APIS, controlador, etc), configuración y puesta a punto para la integración como parte del servicio.

6.8 Planeación de la capacidad

El **LICITANTE** deberá brindar y cumplir una revisión y monitoreo activo de los recursos del ambiente virtual con el objetivo de brindar la adecuada proyección de crecimientos planificados en materia de infraestructura para el fortalecimiento. Como principales fundamentos rectores se analizarán patrones de crecimiento, calendario estacional de procesos de negocio y graficas de tendencia sobre el consumo de los recursos en los ambientes virtuales.

El **LICITANTE** deberá entregar y explicar un reporte de forma quincenal, referente a la capacidad del consumo de recursos en los ambientes virtuales, incluyendo las acciones a ejecutar de forma proactiva para mantener la operación (incremento o decremento de recursos) basadas en las tendencias de consumo estacionales.

7 Unidad de Almacenamiento de Objetos sobre plataforma de nube pública

El **LICITANTE** otorgara un esquema de consumo de almacenamiento de objetos en nube pública con la característica principal de ser escalable a las necesidades del **IMSS**.

El **LICITANTE** brindara una solución integral que asegure la escalabilidad, garantizando la disponibilidad de los datos almacenados, seguridad y el rendimiento en el acceso a los mismos.

La solución propuesta por el proveedor deberá soportar diversos casos de uso, que, con el previo diseño de la infraestructura involucrada pueda ser compatible con los escenarios que el **IMSS** pueda proyectar. Como ejemplo de los escenarios que la plataforma debe ofrecer son: uso para sitios web, aplicaciones móviles, procesos de copia de seguridad y restauración, operaciones de archivado, aplicaciones empresariales. La solución propuesta por el proveedor deberá contar con características de administración fáciles de utilizar que permitan organizar los datos y configurar sofisticados controles de acceso. Así mismo, se deberá ofrecer una disponibilidad del 99,9999 %.

El **IMSS** solicita al **LICITANTE** poder entregar uno de los siguientes esquemas, siendo limitativo a la ejecución de un esquema, pero con la posibilidad de escalar hasta el más demandante

- Esquema 1:
  a. Almacenamiento disponible: 500 TB
     - Cantidad de Peticiones PUT/COPY/POST/LIST soportadas: 1,000,000
     - Cantidad de Peticiones GET/SELECT/Other soportadas: 1,000,000

  b. Transferencia de datos
     - Salida: 2 TB al mes
     - Entrada: 10 TB al mes
- Esquema 2:
  a. Almacenamiento disponible: 750 TB
     - Cantidad de Peticiones PUT/COPY/POST/LIST soportadas: 3,000,000
     - Cantidad de Peticiones GET/SELECT/Other soportadas: 3,000,000
  b. Transferencia de datos
     - Salida: 10 TB al mes
     - Entrada: 50 TB al mes
- Esquema 3:
  a. Almacenamiento: 1 PB
     - Cantidad de Peticiones PUT/COPY/POST/LIST soportadas: 5,000,000
     - Cantidad de Peticiones GET/SELECT/Other soportadas: 5000000
  b. Transferencia de datos
     - Salida: 20 TB al mes
     - Entrada: 100 TB al mes
- Esquema 4:

c. La modalidad de dicho esquema podrá ser la combinación de los esquemas anteriores o en su caso la incorporación de nuevas soluciones de almacenamiento de este tipo las cuales podrán estar vigentes durante la vigencia del contrato.

a) Unidad integral de conmutación de datos y de protección contra amenazas y detección de intrusos

Con la finalidad de obtener la mejor solución de seguridad de la información, el área independiente de punto de control de calidad deberá elaborar el diseño de la arquitectura de seguridad, considerando los elementos necesarios para proporcionar la confidencialidad, integridad y disponibilidad de los activos de tecnologías de información y comunicaciones del **IMSS**. Esta estrategia permitirá consolidar la integración de servicios, funciones, sistemas e infraestructura tecnológica en busca de mayor eficiencia, productividad y economías de escala.

En lo referente a la administración y control de la seguridad informática se requiere el diseño de una arquitectura tecnológica integral que tenga par objetivo proveer infraestructura tecnológica que operen con altos niveles de disponibilidad y eficiencia bajo las mejores prácticas de gestión para las tecnologías de la información y comunicaciones.

Esta arquitectura tecnológica integral se conformará de diferentes plataformas específicas, que deberán trabajar en conjunto de forma transparente y segura, para que el **IMSS** obtenga el mayor beneficio en términos de seguridad de la información en el uso de la tecnología.

Adicionalmente, el **IMSS** requiere que se realicen los protocolos de pruebas, interoperabilidad y validación de todos los componentes que integran la solución de seguridad teniendo un único punto de control de calidad, el cual tiene como objetivo tiene realizar las validaciones correspondientes que permitan cumplir con lo solicitado en el presente documento.

El **LICITANTE** en conjunto con el IMSS realizara las pruebas y validaciones a fin de dar certeza de que estos componentes se encuentran establecidos bajo las condiciones establecidas en el presente anexo. La arquitectura tecnológica integral que fortalecerá la plataforma de seguridad de la información del IMSS se integrará de los siguientes elementos:

i. Unidad integral de Conmutación de Datos

La unidad de componente integral de conmutación de datos 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 y LAN to LAN, redireccionándolos hacia los destinos correspondientes.

El equipamiento propuesto para la 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.

La solución deberá considerar e incluir toda la infraestructura y los insumos necesarios para brindar conectividad a las diferentes aplicaciones del **IMSS** 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 **IMSS** que estarán conectados.

Las características mínimas por incluir son:

- El **LICITANTE** deberá crear al menos una VLAN para lograr la extensión del direccionamiento LAN del **IMSS**, sin embargo, el **IMSS** 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 **LICITANTE** deberá garantizar el flujo de tráfico entre todas las VLAN's que solicite el **IMSS**. Todas las VLAN's deberán ser implementadas con un ancho de banda de al menos 1 GB, por lo que el **LICITANTE** deberá considerar el equipamiento necesario para lograrlo.
- El **LICITANTE** deberá considera que todas las VLAN´s deberán estar debidamente aisladas de otros clientes que tengan servicios en el Centro de Datos contratado actualmente por el **IMSS**, de forma que ningún paquete de datos que fluya sobre la o las VLAN's que se implementen para el **IMSS** viaje a través una VLAN de otro cliente; tampoco estará permitido que paquetes de datos de otros clientes del Posible **LICITANTE** viajen a través de las VLAN's que se implementen para el **IMSS**.
- El **LICITANTE** deberá considerar e incluir el transporte, la conmutación, así como el enrutamiento de paquetes, a conveniencia o solicitud del **IMSS**.
- El **IMSS** 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 **IMSS** tiene el derecho de efectuar en cualquier momento y las veces que considere necesario, las inspecciones físicas en las instalaciones del **LICITANTE**, con la finalidad de verificar el cumplimiento de lo solicitado.
- El **LICITANTE** 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 **IMSS** intercambia de manera segura información con diversas Instituciones.
- El **LICITANTE** deberá integrar todo lo necesario para soportar la recepción de enlaces LAN to LAN (L2L), para generar la conectividad con terceros.

ii. Unidad integral de firewalls de siguiente generación

El **IMSS** requiere el aprovisionamiento de la infraestructura que brinde seguridad perimetral, protección de control de acceso, bloqueo contra ataques dirigidos a las aplicaciones e inspección sobre los paquetes a nivel de aplicación que permita la identificación de patrones de tráfico anómalo.

El **LICITANTE** en conjunto con el IMSS definirán en conjunto la estrategia de implementación de los Firewalls que formara parte de la arquitectura de seguridad y comunicaciones definida en el presente anexo. La solución propuesta deberá estar configura bajo un esquema de alta disponibilidad.

El **LICITANTE** deberá llevar a cabo todas las tareas necesarias para la instalación del equipamiento y el cual se ubicará dentro de su centro de datos.

La solución propuesta deberá estar configurada y funcionando en un esquema de alta disponibilidad deberá ser de siguiente generación de propósito específico; es decir que el equipamiento propuesto deberá estar dedicada a las funcionalidades de firewall, IPS, visibilidad granular y control de aplicaciones y filtrado de contenido web. Adicionalmente, deberá incluir una consola de administración que permita su gestión a

manera de poder administrar y monitorear los logs, manejo de imágenes de software, configuración de alertas y health check, etc. Esta solución permitirá controlar el acceso a la salida a internet, las zonas desmilitarizadas y proporcionará los mecanismos de protección contra amenazas persistentes, del dia zero, detección de intrusos y protección contra malware avanzado. Así mismo, permitirá la publicación segura de los aplicativos y sistemas que el IMSS designe.

El **LICITANTE** deberá de incluir el software (virtualización y sistema operativo) y hardware requerido para la correcta instalación de la(s) consola(s) de administración así mismo el **LICITANTE** podrá instalar las aplicaciones que de acuerdo al dimensionamiento puedan ser virtualizadas en un mismo servidor, sin embargo se deberá de incluir el software de virtualización y/o hipervisor correspondiente así como el switch virtual de hipervisor (con soporte de calidad de servicio, L3, puerto espejo); en cuanto a la conectividad del hardware (servidor), deberá de incluir al menos 2 Interfaces 100/1000 en cobre para la conexión a la red del centro de datos del **LICITANTE**.

El equipamiento propuesto deberá ser nuevo, de última generación y dedicado para las necesidades del **IMSS** y deberá cumplir con las siguientes especificaciones técnicas mínimas de forma enunciativa más no limitativa:

CARACTERISTICA TECNICA	REQUERIMIENTO SOLICITADO	
Características Técnicas de Firewall	Desempeño de Firewall	39 Gbps
	Desempeño de prevención de amenazas	18 Gbps
	Desempeño IPSec VPN	16 Gbps.
	Conexiones por segundo	284,000
	Sesiones Concurrentes	8,000,000
	Configuración en alta disponibilidad	Activo/Activo Activo/Standby
	Modo de Operación en capa 3 (routing)	Incluido
	Soporte NAT	Incluido
	Soporte PAT	Incluido
	Conexiones incluidas VPN Site to Site	4000
	Conexiones incluidas VPN Client to Site	4000
Características de Nueva	Inspección de al menos 1,000 distintas aplicaciones, así como	Incluido

CARACTERISTICA TECNICA	REQUERIMIENTO SOLICITADO	
Generación (NGFW)	de 75,000 de micro aplicaciones	
	Utilización de Inspección Paquetes Profunda (DPI)	Soportado
	Detección y prevención de intrusos (IPS) Filtrado de contenido de la WEB Detección y control de virus Detección y control de amenazas y programas maliciosos Bloquea un rango de amenazas conocidas (como exploits, malware y spyware) a través de todos los puertos independientemente de las tácticas comunes de evasión de amenazas empleadas	Incluido
	Monitoreo centralizado que incluya el licenciamiento para permitir el reporteo, visualización de logs y eventos	Incluido
	Rango de Voltaje en línea	100 - 240V
	Voltaje Normal	100 - 240V
	Conectividad Eléctrica	Se deberá proporcionar los conectores hembra/macho y PDU´s de interconexión eléctrica necesarios.
Características de Enrutamiento	Policy-based routing	Incluido
	Multicast Routing	Incluido
	IGMP (v1, v2)	Incluido
Características Físicas	PIM SM	Incluido
Características Eléctricas	OSPF	Incluido

ANEXOS
DIVISION DE CONTRATOS

CARACTERISTICA TECNICA	REQUERIMIENTO SOLICITADO	
Características de Interfaces	Puertos Físicos 10GE (SFP+)	4 puertos incluidos SR
	Puertos de comunicación	Incluido jumper e interfaz física por puerto incluido
Características de Enrutamiento	Puertos Físicos 10/100/1000 Base-T	4 puertos incluidos
Características IPv6	Puerto Consola	Incluido
Características de Administración y Monitoreo	Dual Stacking firewall	Incluido
	Generación de reporteo de firewall (top services, top sources, top destinations)	Incluido
Características de Reporteo	Generación de reporteo de IPS (Top Attackers, Top Blocked/Unblocked Signatures, Top Signatures)	Incluido
	Generación de reporteo de VPN (Top Bandwidth Users (SSL/IPsec)	Incluido
	WEBGUI Global	Incluido
	WEBGUI dedicado por firewall virtual	Incluido
Características IPv6	Monitoreo de las aplicaciones que cursan la red	Incluido
Características de Administración y Monitoreo	Monitoreo de la actividad web de usuarios en la red	Incluido

CARACTERISTICA TECNICA	REQUERIMIENTO SOLICITADO	
Protección de Ataques Conocidos Características VPN	Permita la generación de contraseña de acceso por firewall virtual	Incluido
	Visualización Número de sesiones en tiempo real por firewall virtual.	Incluido
	Visualización en Uso de CPU en tiempo real del firewall	Incluido
	Visualización de Actividad de eventos en consola en tiempo real por firewall virtual	Incluido
	Interfaz de administración por CLI en consola	Incluido
	Interfaz de administración por CLI mediante SSH por firewall virtual.	Incluido
	Interfaz de administración por CLI mediante TELNET por firewall virtual	Incluido
	Administración por CLI de cada instancia de firewall virtual	Incluido
	Múltiples servidores de SYSLOG	Incluido
	Notificación por medio de correo electrónico	Incluido
	SNMPv2	Incluido
	SNMPv3	Incluido
	Logging Remoto	Incluido
	Monitoreo de Túneles VPN	Incluido
	Protección a ataques FLOOD	Incluido
	Protección a ataques fragmentados de ICMP	Incluido

CARACTERISTICA TECNICA	REQUERIMIENTO SOLICITADO	
Protección de Ataques Conocidos	Protección a ataques de escaneo de puertos	Incluido
	Protección a ataques de Denegación de Servicio (DoS)	Incluido
	Protocolo de encripción 3DES	Incluido
	Protocolo de encripción AES	Incluido
	Autenticación MD5	Incluido
	Autenticación SHA-1	Incluido
	Grupos DIFFIE HELLMAN	Incluido
	IPSEC NAT Transversal	Incluido
	Configuración Hub & Spoke en VPN Site to Site	Incluido
Certificaciones	SOC2. FIPS 140-2, Common Criteria, NCSC Foundation Grade Certification, ANSSI top-level certification.	incluido
Servicios Profesionales	Diseño (plan migración de las actuales configuraciones de seguridad), optimización, instalación, configuración y puesta en operación.	Incluido

iii. Unidad integral de protección contra ataques DDOS

El **IMSS** requiere solución de seguridad para la protección contra ataques de denegación de servicio distribuido (DDoS). La tecnología requerida por el **IMSS** deberá de propósito específico; es decir que la tecnología ofertada por el **LICITANTE** deberá estar dedicada en funcionalidad a la protección de ataques DDoS.

El **LICITANTE** deberá aprovisionar toda la infraestructura necesaria la cual deberá ser nueva y cumplir al 100% con las características mínimas necesarias descritas en el presente documento para ofrecer una solución de protección contra ataques DDoS.

El **LICITANTE** deberá llevar a cabo todas las tareas necesarias para la instalación del equipamiento y el cual se ubicará dentro de su centro de datos.

La tecnología requerida por **IMSS** deberá cumplir con una arquitectura diseñada y desarrollada por el fabricante con el único y exclusivo propósito de mitigar los ataques DDoS. La tecnología requerida deberá estar diseñada para que sea instalada en el borde de las salidas a internet con las que cuenta el **LICITANTE**.

El **LICITANTE** en conjunto con el IMSS definirán en conjunto la estrategia de la solución de la protección contra ataques DDoS que formara parte de la arquitectura de seguridad y comunicaciones definida en el presente anexo.

El **LICITANTE** deberá proporcionar una solución basada en una arquitectura dedicada a la mitigación de ataques de denegación de servicio distribuido. La cual deberá incluir diversos modos de operación monitor (pasivo) y activo. Lo anterior, nos permitirá generar una línea base del comportamiento del tráfico, así como la detección oportuna de amenazas contra los activos del IMSS que estén publicados dentro del centro de datos del **LICITANTE.**

El **LICITANTE** deberá realizar una estrategia de implementación de la solución basada en las mejores prácticas del fabricante de la solución propuesta. Es decir, la estrategia propuesta deberá estar basada en las guías oficiales de implementación del fabricante de la solución.

Adicionalmente, la solución de protección contra ataques DDoS deberá cumplir al menos con lo siguiente:

- Protección de paquetes que no son válidos (incluidos los controles de encabezados IP malformados, fragmentos incompletos, checksum IP erróneos, fragmentos duplicados, fragmentos muy largos, paquetes pequeños, paquetes TCP pequeños, paquetes UDP pequeños, paquetes ICMP pequeños, checksums TCP/UDP erróneos).
- Protección de ataques de inundación (flood) TCP.
- Protección de ataques de inundación (flood) UDP.
- Protección de ataques de inundación (flood) ICMP.
- Bloquear tráfico originado por botnets.
- Detectar y bloquear las inundaciones de SYN's TCP.
- Bloqueo de ataques en HTTP.
- Actualizar automáticamente las firmas o patrones de protección de ataques periódicamente a intervalos configurables.
- Permitir que los parámetros de protección sean cambiados mientras la protección está ejecutándose.
- El sistema debe tener la opción de bloquear por país de origen.
- Bloqueo de ataques en DNS.
- Mitigar los ataques volumétricos de DDoS en la nube en conjunto con los proveedores de servicio (ISP).
- Bloqueo de ataques IPv6.

iv. Unidad Integral de firewall de aplicaciones web

EL LICIANTE deberá de integrar una solución que contenga técnicas de detección y mitigación para frustrar los ciberataques más sofisticados y los detenga incluso antes de que lleguen a los servidores, este la solución deberá de aparecer con un porcentaje mayor al 99.80% de eficacia en una comparativa (Web Application Firewall Comparative Analysis) de nss labs y ser calificado como líder, dentro de su reporte anual, por la firma consultora y de investigación Gartner. La solución deberá cumplir de forma enunciativa, más no limitativa con las características que a continuación se enlistan:

- La solución deberá contar con un modo aprendizaje para rastrear cambios continuos dentro de las aplicaciones web del **IMSS**, deberá reconocer dichos cambios y simultáneamente protegerlas. La solución propuesta deberá soportar lo siguiente:
  - La solución de firewall de aplicación web y el monitoreo de actividades para el firewall de inspección de archivos deberá soportar el licenciamiento para la protección de aplicaciones web en paquetes de 10 aplicaciones web, los cuales podrán ser integrados de acuerdo a las necesidades del IMSS.
  - Aprender los valores aceptables para los campos de ingreso de datos con base en el registro de la actividad.
  - De los valores aprendidos, deberán ser utilizados como la configuración inicial sobre la que se revisarán los datos ingresados en el modelo positivo de seguridad.
  - En modo aprendizaje, deberá aprender la estructura y elementos de la aplicación (directorios, url´s, parámetros, cookies) y el comportamiento esperado del usuario (longitud del valor esperado, caracteres aceptados, si el parámetro es de sólo lectura o editable por el usuario) y esta información deberá estar disponible para automatizar la configuración del modelo positivo de seguridad.
  - La configuración aprendida deberá ser accesible y modificable para el administrador del dispositivo.
  - La solución deberá correlacionar múltiples eventos de seguridad para distinguir tráfico deseado del tráfico inadecuado.
  - La solución deberá permitir la modificación de reglas de seguridad. Los administradores deberán poder definir reglas para el modelo de seguridad positivo o negativo y deberán crear reglas de correlación con múltiples criterios.
  - 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 el HTTP Request o el Response por parte del servidor Web
    - Tipo de archivo siendo transmitido en cualquier sentido
    - Host o dominio accedido
    - Métodos HTTP usados
    - Número de ocurrencias en intervalos de tiempo definidos
    - La existencia o contenido de cualquier Parámetro web
    - Por el protocolo usado, HTTP o HTTPS
    - IPs de origen y destino
    - Por la existencia o contenido de Cookies o el identificador de Sesión
    - Response Code y Headers en el Response HTTP por parte del servidor Web
    - Hora del Día
    - Por usuario firmado en el aplicativo web

- User-Agent
- Referer-URL
- Tiempo de respuesta o tamaño de la respuesta HTTP

- La solución deberá contar con el modo de instalación proxy transparente.
- La solución deberá cubrir todas las vulnerabilidades expresadas en el OWASP Top Ten más reciente.
- La solución deberá cumplir con todos los criterios de evaluación del WAFEC definidos por el ***Web Application Security Consortium***.
- La solución deberá soportar la integración con seguridad para base de datos, del mismo fabricante, para ofrecer seguridad de extremo a extremo; desde internet hasta la base de datos sin ningún cambio en la aplicación web. La seguridad integrada de la base de datos deberá proteger contra ataques conocidos a las bases de datos, deberá también tener capacidad de monitorear y controlar la actividad de la base de datos.
- La solución deberá proporcionar el bloqueo de direcciones IP, sesiones TCP o usuarios de la aplicación web.
- La solución deberá proteger tanto las aplicaciones Web HTTP, como las aplicaciones web SSL y HTTPS.
    - La solución deberá tener la capacidad de recibir y utilizar los certificados y pares de llaves público/privadas para los servidores web protegidos.
    - La solución deberá descifrar el tráfico SSL, de las aplicaciones web, entre el cliente y el servidor y re-encriptarlo antes de su reenvío.
    - En los modos puente (bridge) o sniffer, la solución deberá poder descifrar el tráfico SSL para inspección, sin terminar o cambiar la conexión HTTPS.
    - La solución deberá tener la capacidad de proteger aplicaciones web que incluyan el contenido de servicios web (xml). La protección XML deberá contar con mecanismos automatizados de aprendizaje, similares a los de la protección de aplicaciones web.
    - La solución deberá soportar la conmutación de datos por error o failover.
    - La solución deberá soportar las opciones fail-open y fail-closed.
- La solución deberá contar con funcionalidades que permitan:
    - Rastrear e identificar las fuentes de los ataques originadas desde proxies anónimos, direcciones IP maliciosas, botnets y sitios de phishing.
    - Actualizar las fuentes de ataque para identificar y bloquear el tráfico malicioso.
    - Ajustar dinámicamente las políticas de seguridad con base en la identificación de las fuentes de ataque o de las fuentes que denoten actividad sospechosa.
    - Bloquear solicitudes de acceso basado en la reputación de la fuente del tráfico, como direcciones IP conocidas por su comportamiento malicioso por Botnet, DDoS, Phishing o redes de Anonimización (TOR y Proxies Anónimos).
    - Bloquear solicitudes de acceso basado en el país de origen de la conexión.
    - Realice un análisis automático de distribución de alertas en relación al país de origen, con opción a representar la información a través de un mapa mundial
    - Detallar y analizar los eventos de seguridad ocurridos, orígenes y método del ataque, dirección IP y localización geográfica del ataque."
- La solución deberá:
    - Inspeccionar y monitorear todos los datos http y la aplicación, incluyendo, los encabezados http, campos de formularios, y el cuerpo http.

- Inspeccionar las peticiones y respuestas http.
- Tener la habilidad de decodificar datos a su mínima expresión a partir de diferentes sistemas de encoding Web y validarla.
- Validar todos los tipos de datos ingresados, incluyento URLs, formularios, cookies, cadenas de queries, campos y parámetros ocultos, métodos http, elementos XML y acciones SOAP.

v. Unidad Integral de firewall de bases de datos

El **IMSS** requiere de una solución contra las amenazas hacia las bases de datos, que monitoree la actividad local en todos los servidores que: las contengan, alerte y detenga el comportamiento malicioso en tiempo real, además de que funcione en ambientes virtualizados o servicios distribuidos en red, la cual deberá contar con las siguientes características:

- La solución deberá contar con tecnología de auto-aprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo schemas, objetos, tablas; sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario; todo esto para el establecimiento de un baseline de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.
- La solución deberá incluir al menos el licenciamiento y soporte que sea compatible con las plataformas de Windows, Linux y Unix.
- Para el caso de crecimiento de la solución de firewall de bases de datos, este deberá estar soportado únicamente mediante paquetes de licenciamientos de al menos 10 instancias de bases de datos.
- La solución deberá proporcionar protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.
- La solución deberá generar reportes y tendencias en tiempo real, así como permitir la modificación de los mismos.
- La solución deberá contar con facilidades o herramientas analíticas para la conducción de análisis forense cuando sea reportado algún incidente.
- La solución no deberá requerir el instalar agentes de software en los servidores a monitorear, pero deberá tener la opción en caso de ser necesario.
- La solución deberá funcionar independiente a la activación de la auditoría nativa de la base de datos.
- La solución deberá ser transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
- La solución deberá ser capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de comunicación, y configuración de seguridad, sin importar el sistema operativo sobre el que se encuentren instaladas.
- La solución deberá realizar una evaluación exhaustiva de los riesgos de la infraestructura objetivo a diferentes niveles/capas de la infraestructura de base de datos incluyendo:
  - Cuestiones de configuración de la base de datos tales como nivel de parcheo, configuración de las cuentas de usuario, evaluación de la fortaleza de las contraseñas, vigencia de contraseñas.
  - Cuestiones de configuración de la plataforma, incluyendo configuración del sistema operativo de los servidores que soportan el software de base de datos.

- La solución deberá de poder realizar descubrimientos automatizados en la red para identificar nuevas bases de datos siendo habilitadas, ya sea a nivel de servidor o puertos habilitados en servidores conocidos.
- La solución deberá tener la capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo a las políticas de negocio. Las definiciones de tipo de dato deberán poder crearse de manera flexible y granular.
- La solución deberá proveer una solución de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.
- La solución deberá apoyar en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y control de cambios.
- La solución deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
- La solución deberá monitorear e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, ligas, stored procedures, entre otros.
- La solución deberá hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.
- La solución deberá tener capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.
- La solución deberá proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.
- La solución deberá manejar reglas y políticas tan amplias o granulares como se requieran y deberán poder ser construidas automáticamente o manualmente y deberán poder ser actualizadas, igualmente, de forma manual o automática.
- Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:
    - Número de registros a regresar por la consulta (SQL Query)
    - Número de registros afectados
    - Tipo de datos accesado (financiero, recursos humanos, inventarios, o cualquier definición personalizada)
    - Acceso a datos marcados como sensibles
    - Base de Datos, Schema, Instancia, Tabla y Columna accedida
    - Estado de autenticación de la sesión
    - Usuario y/o Grupo de Usuarios de Base de Datos conectado
    - Usuario conectado en la capa aplicativa, a diferencia del usuario conectado a la DB
    - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier personalización por expresiones regulares)
    - Logins, Logouts, Queries
    - IPs de origen y destino
    - Nombre de Host origen, Usuario firmado en el Host origen
    - Aplicación usada para la conexión a la base de datos
    - Tiempo de respuesta/procesamiento del query
    - Errores en el manejador de SQL
    - Número de ocurrencias en intervalos de tiempo definidos
    - Por operaciones básicas (Select, Insert, Update, Delete)
    - Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export)
    - Por Stored Procedure o Function utilizada
    - Si existe ticket asignado de cambios

  - Hora del Día
- La solución deberá identificar individualmente a los usuarios finales que realicen actividades mediante aplicaciones, aún si utilizan mecanismos comunes de comunicación entre la aplicación y la base de datos, esta actividad no deberá implicar la modificación de la aplicación y/o de la base de datos.
- La solución debe posibilitar los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.
- La solución deberá asociar y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son indicativos de una potencial violación de seguridad.
- La solución deberá proteger contra ataques SQL y no-SQL (como buffer overflow)
- La solución deberá correlacionar actividad en base de datos con actividad de aplicaciones web para entender detalladamente como los usuarios están accediendo datos privilegiados sin necesidad de alterar la aplicación web.
- Considerados de emergencia para potenciales violaciones de la información que incluyan, enunciativa mas no limitativamente:
  - Altos volúmenes de acceso a datos sensibles más allá de lo habitual.
  - Acceso a datos inusual para cierta hora del día.
  - Acceso a datos desde una ubicación (física) desconocida.
  - Acceso a datos utilizando aplicaciones/herramientas no autorizadas.
- La solución debe manejar una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.
- La solución debe tener facilidades de Archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP)
- La solución deberá contar con Políticas, Reportes, Alertas, Objetos Sensibles, y Transacciones pre-identificadas y pre-configuradas para trabajar con las siguientes plataformas empresariales: Oracle EBS, Peoplesoft, SAP, SQL, entre otras
- La solución deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.
- La solución deberá analizar los eventos generados desde diferentes bases de datos. El análisis deberá contemplar los siguientes criterios:
  - Deberá mostrar el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos.
  - Deberá contar con un sistema de correlación basado en la dirección de los ataques. Deberá determinar si los ataques provienen desde dentro de la organización hacia afuera de la misma o viceversa.
  - Deberá realizar una correlación automática y en tiempo real de eventos, vulnerabilidades y bases de datos.
  - Deberá ejecutar una correlación que permita identificar usuarios de aplicación asociados con consultas –y determinadas actividades– en bases de datos específicas sin necesidad de alterar aplicaciones o instalar API's.
  - Deberá correlacionar eventos como número de errores inusuales de sentencias de SQL o al momento de hacer login a las bases de datos.
- La solución debe permitir el manejo de alarmas y notificaciones –en tiempo real– para los eventos de correlación mencionados anteriormente.
- La solución debe tener la capacidad de monitorear aplicaciones web en la misma solución, ofreciendo una visibilidad, seguridad y control desde el usuario web hasta la base de datos.

- La solución deberá contar con un módulo de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de las mismas.
- La solución deberá soportar y aplicar simultáneamente un modelo de seguridad positivo y negativo.
- El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que deberá además cumplir con las siguientes especificaciones:
    - Deberá bloquear las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
    - Deberá incluir una lista pre-configurada y detallada de las firmas de ataque.
    - Deberá permitir la modificación o adición de firmas por el administrador.
    - Deberá permitir la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
    - Deberá detectar ataques conocidos en múltiples niveles, incluyendo, la red, sistemas operativos, software del servidor web y ataques a nivel de aplicación.
- La solución deberá soportar Gateway clúster a nivel de los agentes de monitoreo de Bases de Datos, es decir que los agentes estarán asignados a un Gateway y podrán moverse automáticamente o manualmente según sea el caso sin necesidad de volver a registrar el agente con el Gateway o realizar alguna acción en el servidor en el cual se encuentra instalado el agente.
- La solución debe proporcionar un proceso de instalación, actualización y gestión de cambios centralizada, segura y ágil para los Agentes; la cual debe proporcionar una visión completa de todas las actualizaciones disponibles para los componentes de la solución de protección de Bases de Datos.
- La solución deberá notificar cuando se encuentre disponible una nueva versión de Agente.
- El despliegue y la instalación centralizada de parches y actualizaciones a componentes solo deberá ser realizada por usuarios con los privilegios necesarios y administradores de la herramienta.
- La solución deberá proporcionar información del tráfico enviado de los Agentes a los Gateways, identificando actividades de Bases de Datos que no son necesarias monitorear; permitiendo a los administradores de la solución generar reglas de exclusión para reducir el consumo de recursos en el servidor.
- La solución deberá contar con la opción de reducir el tráfico entre la comunicación entre el Agente y el Gateway utilizando métodos de comprensión de datos.
- La solución deberá proporcionar la opción de enmascarar la información personal que se despliega atreves de la interfaz de administración, además deberá contar con la opción de desenmascarar esta información dependiendo los privilegios de cada usuario.

8 Unidad Integral de Balanceo de Cargas en Comunicaciones

El IMSS requiere la solución de Balanceo de carga L4-L7 para aplicaciones Web o equivalente y su información inherente. La infraestructura propuesta deberá cumplir con las siguientes especificaciones técnicas mínimas:

- La solución de balanceo de carga propuesta deberá estar en alta disponibilidad.
- El equipamiento propuesto deberá ser de propósito específico; es decir que la tecnología propuesta deberá estar dedicada en funcionalidad para el balanceo de carga de capas 4 a capa 7 del modelo OSI, por lo que no se aceptaran dispositivos con tecnologías cortafuegos (firewalls), sistemas de

prevención y detección contra intrusos (IPS) y las variantes o combinaciones como firewall de gestión unificada de amenazas (Unified Threat Management o UTM, por sus siglas en inglés), firewalls de próxima generación (Next Generation Firewall o NGFW, por sus siglas en inglés), sistemas de prevención de próxima generación (Next Generation IPS o NGIPS por sus siglas en inglés), firewall de aplicación (Web Application Firewall o WAF, por sus siglas en inglés).

- La tecnología requerida deberá cumplir con la arquitectura diseñada y desarrollada por el fabricante con el único y exclusivo propósito de balanceo de cargas.
- Adicionalmente, la solución deberá soportar la funcionalidad de alta disponibilidad para obtener un mejor nivel de disponibilidad.
- El equipamiento propuesto deberá soportar al menos 650,000 de peticiones (capa 7 del modelo OSI) por segundo.
- El equipamiento deberá soportar al menos 250,000 conexiones por segundo.
- El equipamiento deberá tener un desempeño de 10 Gbps.
- El equipamiento propuesto deberá contar con fuente de poder redundante

El LICITANTE deberá aprovisionar toda la infraestructura necesaria la cual deberá ser nueva y cumplir al 100% con las características mínimas necesarias descritas en el presente documento para ofrecer la solución de balanceador de cargas.

9 Unidad de Componente Integral de Punto Neutro

El **IMSS** requiere establecer comunicación desde diferentes ubicaciones o localidades remotas hacia el centro de datos ofertado, donde podrán converger distintos carrier's. En este punto de la red, tendrá que proporcionar a través de su infraestructura de red LAN el transporte de datos, video y voz que se reciban de los distintos **LICITANTES** de enlaces de comunicación.

Esta red, será responsable de alojar la acometida del servicio de Internet con la que hoy cuenta el **IMSS**, 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 para cumplir en cuanto a capacidad, funcionalidad, operación y disponibilidad de la solución propuesta:

Deberá incluir interfaces físicas redundantes, con infraestructura de comunicaciones en alta disponibilidad dedicada, con capacidad instalada para operar al menos lo siguiente:

- 48 interface RJ45 en cobre a velocidad de al menos 1 Gbps,
- 48 interface Ópticas a velocidad 1 o 10 Gbps.
- 6 clases de Servicio MPLS.
- Infraestructura "Nonblocking".
- Interconexión de componentes en Malla con enlaces de alta capacidad 40 y 100 Gbps.
- Capacidad de conectar al menos 35 Redes MPLS.
- Capacidad de conectar al menos 35 Enlaces Punto a Punto. (ruteables).
- Capacidad de conectar al menos 35 Enlaces L2L.
- Capacidad para recibir 1000 usuarios de VPN "site to site" en IPSEC de diferentes fabricantes de equipo.
- Capacidad de recibir 1000 usuarios de VPN "cliente to site" en IPSEC con dispositivos móviles.

- Monitoreo continuo de todos los componentes de esta solución, así como de los servicios integrales de comunicaciones.
- Acceso al centro de datos con trayectoria redundante diferentes.
- 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.

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 serán las estipuladas por el Centro de Datos del **LICITANTE** donde será alojada la infraestructura del **IMSS**.

El equipamiento debe soportar recibir al menos los siguientes servicios:

1 enlace redundante a Internet con un ancho de banda inicial de 1 Gbps y un máximo de 10 Gbps.

- Deberá recibirse con Interfaces físicas necesarias en cobre (RJ45) u ópticas (MTRJ) compatibles con la velocidad al menos de 1 Gbps y de 10 Gbps.
- En caso de requerirse uno o más tendidos nuevos o reubicaciones de cableado ya sea UTP o fibra óptica, deberá proporcionarse con cables categoría 6 y multimodo respectivamente, las Interfaces en cobre (RJ45) u ópticas (MTRJ) que soporten al menos la velocidad al menos de 1 Gbps y de 10 Gbps.
- La Infraestructura de equipo de comunicaciones deberá proporcionarse en alta disponibilidad.

2 enlaces LAN to LAN redundantes con un ancho de banda inicial de 1 Gbps y un máximo de 10 Gbps.

- Deberá recibirse con Interfaces físicas necesarias en cobre (RJ45) u ópticas (MTRJ) compatibles con la velocidad al menos de 1 Gbps y de 10 Gbps.
- En caso de requerirse en Punto Neutro uno o más tendidos nuevos o reubicaciones de cableado ya sea UTP o fibra óptica, deberá proporcionarse con cables categoría 6 y multimodo respectivamente, las Interfaces en cobre (RJ45) u ópticas (MTRJ) que soporten al menos la velocidad al menos de 1 Gbps y de 10 Gbps.
- La Infraestructura de equipo de comunicaciones deberá proporcionarse en alta disponibilidad.

2 enlaces MPLS redundantes con un ancho de banda inicial de 500 Mbps y un máximo de 10 Gbps.

- Deberá recibirse con Interfaces físicas necesarias en cobre (RJ45) u ópticas (MTRJ) compatibles con la velocidad al menos de 1 Gbps y de 10 Gbps.
- En caso de requerirse en Punto Neutro uno o más tendidos nuevos o reubicaciones de cableado ya sea UTP o fibra óptica, deberá proporcionarse con cables categoría 6 y multimodo respectivamente, las Interfaces en cobre (RJ45) u ópticas (MTRJ) que soporten al menos la velocidad al menos de 1 Gbps y de 10Gbps.
- La Infraestructura de equipo de comunicaciones deberá 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 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.

10 Unidad de Enlaces dedicados con una capacidad de 5 Gbps

El **LICITANTE** a través del establecimiento e implementación del Enlace LAN to LAN (L2L) deberá lograr una extensión del direccionamiento LAN del sitio del **IMSS** 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 al menos son las siguientes:

- Interfaces físicas 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.
- Direccionamiento IP privado con la validación del **IMSS.**
- Capacidad de conectar al menos 1 (un) enlace "LAN to LAN" con una capacidad de 5 Gbps.
- Monitoreo de red y análisis de tráfico.
- Acceso al centro de datos con doble trayectoria.
- Niveles de disponibilidad mensual de 99.90%.
- Infraestructura dedicada.
- El apego a las políticas de acceso físicas serán las estipuladas por el **LICITANTE** en acuerdo con el **IMSS**.
- La solución deberá de recibir en una capa extra de seguridad por medio de un clúster de firewalls que permita realizar DMZ independientes por enlace con el fin de acotar mediante políticas de "firewall" los accesos por puertos TCP/IP a las aplicaciones de la contratante.
- El **PROVEEDOR** 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.
- Se contempla un enlace del centro de datos ubicado en la ciudad de Monterrey hacia el centro de datos del nuevo **LICITANTE.**
- Se contempla dos enlaces del centro de datos del actual **LICITANTE**, al centro de datos del nuevo **LICITANTE.**

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.

11 Unidad de Soporte

El soporte deberá contar con las siguientes características mínimas:

- El LICITANTE deberá recibir solicitudes de servicio por parte del IMSS vía telefónica y correo electrónico, mediante un punto único de contacto (Centro de soporte del proveedor). El tiempo de respuesta para el seguimiento de solicitudes deberá ser inmediato, el LICITANTE deberá contar con una matriz de escalamiento. El centro de soporte del LICITANTE ganador deberá contar con disponibilidad ininterrumpida para la recepción de solicitudes de soporte en horario de 7x24.
- El IMSS podrá realizar solicitudes de soporte para obtener asistencia telefónica, o por correo electrónico por parte del proveedor, provisto a través de personal certificado.
- En caso de que el soporte técnico requerido esté relacionado con fallas de hardware, el LICITANTE deberá remplazar sin costo alguno para el IMSS el equipo dañado por uno de iguales o mejores características, para cubrir los niveles de servicio solicitados.

En caso de falla de hardware/software el LICITANTE deberá estar disponible en un horario de 7x24 para el remplazo de las partes dañadas con un tiempo de solución no mayor a 4 horas una vez que el IMSS haya reportado la falla al centro de atención del proveedor, el LICITANTE tendrá un tiempo no mayor a 15 minutos para el registro del ticket correspondiente, así como su seguimiento con la mesa de servicio del IMSS.

12 SERVICIO DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN

El **LICITANTE** deberá habilitar, implementar, configurar, administrar, operar, monitorear y soportar la plataforma de respaldos siendo de manera enunciativa más no limitativa, incluyendo los siguientes conceptos:

- Niveles de protección tipo RAID 5 o superior y contar con discos hotspare, que evite pérdida de datos.
- Garantizar el aprovechamiento de las redes de conectividad LAN y SAN para las funciones de respaldos.
- Contar con conectividad FC y Ethernet, con soporte da los diversos medios de almacenamiento ofertados, con funciones de deduplicación (compresión) de los datos a respaldar.
- Garantizar la disponibilidad y su mantenimiento no disruptivo dando continuidad al servicio de respaldo y restauración de la información.
- Utilizar algoritmos de deduplicación de datos para almacenar la información, que cumplan las siguientes características:
  - La deduplicación de los datos respaldados debe ser "en línea", sin que represente este proceso una tarea posterior de la ejecución del mismo.
  - El mencionado proceso de deduplicación no deberá representar un espacio adicional temporal.
  - El proceso de deduplicación deberá distribuirse en el origen y en el destino a través de los protocolos Ethernet y FC en una red local independiente con un componente de comunicaciones dedicado, de manera que este proceso no afecte la operación de la plataforma virtualizada.
- Soportar el escenario de recuperar la información en un sitio alterno en caso de que el sitio principal presente algún problema que impida la operación.
- El **LICITANTE** deberá establecer de manera conjunta con el Instituto, un esquema de respaldos y restauración de la información, en los servicios de las bases de datos y de carpetas (datos no estructurados) contenidas en la plataforma de virtualización.
- El respaldo deberá considerar el respaldo en línea ("En caliente") del total de las bases de datos.

- El respaldo deberá hacerse con periodicidad diaria, semanal y mensual de conformidad a lo definido en la solicitud de respaldo y restauración definida por el Instituto.
- Los respaldos diarios tendrán una retención de 7 días, los semanales de 4 semanas, los mensuales de 3 meses y el anual de 1 año o en su caso, los que se determinen por las áreas de negocio del Instituto.
- Los respaldos deberán realizarse en medios externos a la plataforma de virtualización, siendo posible la utilización de medios magnéticos o similares como almacenes mecánicos (discos duros) integrados en plataformas de almacenamiento.
- El LICITANTE deberá contar con una cintoteca, al interior de su Centro de Datos, así como una cintoteca externa de respaldo, para lo cual el Instituto definirá las políticas de respaldo a seguir.
- La restauración deberá poder hacerse en forma completa e incluso por elemento, por ejemplo se deberá poder recuperar un solo archivo de una carpeta o se deberá poder recuperar una sola tabla de una base de datos (excepto para los contenedores).
- La restauración no deberá encimar o sobrescribir información que en esos momentos esté en línea, por consiguiente deberá permitir al personal del **IMSS** copiar de forma personalizada la información recuperada.
- Permitir la replicación de datos entre dos o más equipos a través de la WAN y la replicación debe satisfacer los siguientes puntos:
  a. Replicar datos deduplicados: es decir la replicación debe ocurrir después de los proceso de deduplicación con el objeto de reducir la cantidad de datos a enviar por el enlace WAN y por ende demandar un menor ancho de banda para el proceso.
  b. La replicación debe de poderse efectuar de forma bidireccional, es decir de un equipo local a otro equipo remoto y viceversa

El LICITANTE deberá entregar de forma diaria, un reporte de la ejecución de los respaldos en el cual identifique los exitosos de los fallidos. En caso de falla recurrente (3 ocasiones consecutivas) del mismo proceso de respaldo sin análisis ni ejecución de medidas correctivas, será causa de la aplicación de deductivas.

La solución que brinde el **LICITANTE** deberá incluir todos los componentes físicos y lógicos necesarios para su operación a fin de cumplir con los niveles de servicio establecidos.

En caso de falla de algún componente del equipo utilizado, el contenido almacenado debe poder regenerarse utilizando niveles de protección adecuada para el servicio.

13 SERVICIO DE OPERACIÓN EN INFRAESTRUCTURA DE SEGURIDAD INFORMÁTICA

13.1 Seguridad Lógica

13.1.1 Diseño de la Arquitectura de la Seguridad.

Con la finalidad de obtener los mejores servicios y mejores prácticas, el **LICITANTE** deberá elaborar un diseño de la arquitectura del servicio de seguridad considerando los elementos primordiales para proporcionar la confidencialidad, integridad, y disponibilidad de los activos tecnológicos de TI y comunicaciones del **IMSS**.

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

El diseño de la arquitectura tecnológica integral está conformado componentes de seguridad y un Centro de Operación de Seguridad (SOC), que rigen a los elementos tecnológicos de forma congruente para que el **IMSS** tenga un mayor beneficio y garantía en términos de seguridad de la información.
La arquitectura está compuesta al menos, por los siguientes componentes:

- Firewall.
- DDoS.
- Redes Privadas Virtuales.
- Filtrado de Contenido Web.
- AntiSPAM.
- Web Application Firewall (WAF).
- Database Firewall.
- Centro de Operación de la Seguridad (SOC)

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

13.1.2 Pruebas y validación

El **IMSS** requiere un servicio de pruebas y validación mediante un área independiente de la operación del servicio de seguridad, a fin de garantizar las mejores prácticas y el buen funcionamiento de los servicios tecnológicos.
El **LICITANTE** del servicio deberá integrar un área independiente a la que instala y opera el servicio de seguridad cuya función será la de ser un punto calidad de los servicios cuyo objetivo será validar que los mismos cumplan con los requerimientos y niveles de servicio solicitados por el **IMSS**.

El **IMSS** solicitara la realización de pruebas a las diferentes arquitecturas del servicio a fin de revisar que los diferentes componentes tecnológicos de los servicios de seguridad operen bajo las mejores prácticas de la gestión para las tecnologías de la información y telecomunicaciones.

13.1.3 Análisis de Vulnerabilidades

El **IMSS** requiere de un servicio que permita ejecutar análisis técnicos especializados sobre los activos de infraestructura de procesamiento y redes que permitan identificar vulnerabilidades nuevas y conocidas.
El **LICITANTE** de servicios deberá cumplir al menos con las siguientes funcionalidades operativas:

a. Capacidad para integrarse al menos dos herramientas que permitan complementar los análisis de vulnerabilidad ejecutados.
b. Capacidad para identificar los servicios a analizar incluyendo el número de equipos involucrados y la versión de las plataformas de los sistemas.
c. Identificación de vulnerabilidades documentadas en organismos internacionales como el CVE (Common Vulnerability Exposures).
d. Identificación de configuraciones por omisión.
e. Capacidad para elaborar un reporte técnico y ejecutivo donde se describa un riesgo asociado a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP.

f. Capacidad para integrar un proceso-procedimiento de implementación de las medidas de remediación y recomendaciones realizadas, así como el integrar soporte técnico en la solución de los problemas presentados.
g. Se dispondrá un número ilimitado de eventos para realizar procesos de análisis de vulnerabilidades bajo demanda conforme a las necesidades operativas.
h. Capacidad para determinar el grado de vulnerabilidades ante técnicas de ataque como:
    - SQL Inyection.
    - Cross Site Scripting.
    - Cross Site Request Forgery.
    - Sensitive Data Exposure.
    - Security Misconfiguration.
    - Broken Authentication and Session Management.

13.1.4 Pruebas de Penetración.

El **IMSS** requiere de un servicio que permita realizar unas series de pruebas de penetración sobre la infraestructura con el fin de buscar fallas o debilidades en la seguridad de los sistemas. Todas las pruebas de penetración deberán ser realizadas con herramientas especializadas, así como por ingenieros calificados.
El **LICITANTE** del servicio deberá de cumplir con al menos las siguientes funcionalidades operativas:

a) Identificación de los servicios o activos de información que se analizarán, incluyendo el número de los equipos involucrados y versión de las plataformas.
b) Identificación de vulnerabilidades y malas prácticas de configuración.
c) Explotación vulnerabilidades a los sistemas mediante las debilidades de seguridad detectadas.
d) Evaluación de vulnerabilidades de al menos los siguientes rubros:
    - Autenticación y autorización.
    - Intentos ilimitados de inicio de sesión.
    - Insuficiente autenticación.
    - Insuficiente autorización.
    - Gestión de Sesión.
        - ✓ Predicción de sesión o trabajo.
        - ✓ Secuestro de sesión.
        - ✓ Reproducir sesión.
        - ✓ Expiración de sesión insuficiente.
    - Inyección de Código.
        - ✓ Inyección de comandos al sistema operativo.
        - ✓ Inyección de SQL.
        - ✓ Cross Site Scripting.
        - ✓ Inyección LDAP.
        - ✓ Inyección HTML.
        - ✓ Parameter Tampering.
        - ✓ Coockie Poisoning.
        - ✓ Hidden Field Manipulation.
    - Criptografía.
        - ✓ Fortaleza del algoritmo.
        - ✓ Gestión de llaves.
    - Ataques lógicos.
        - ✓ Abuso de funcionalidades.

- ✓ Input Field Validation Checking.
- o Protección de Datos.
  - ✓ Transporte.
  - ✓ Almacenamiento.
- o Divulgación de información.
  - ✓ Indexado de directorio.
  - ✓ Path Transversal.
  - ✓ Manejo inseguro de errores.
  - ✓ Comentarios HTML.

13.1.5 Análisis Forense.

El **IMSS** requiere un servicio de análisis de incidentes de seguridad para determinar y documentar en que consistió el evento a través de la integración de registros o bitácoras que permitan obtener indicios de incidentes y su relación en el tiempo.

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

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

13.1.6 Correlación de Eventos.

El **IMSS** requiere de un servicio de seguridad que maneje, analice y explote las bitácoras de los dispositivos de seguridad con la finalidad de conocer exactamente que pasa en distintos puntos de la red de forma centralizada y eliminar falsos positivos generados. Se deberá de contar con una solución tecnológica para la administración de eventos e información de seguridad necesaria para el monitoreo, análisis, administración y reporte de eventos de seguridad de la información, que tengan como resultado proveer los mecanismos de identificación de incidentes y riesgos potenciales en la infraestructura y servicios tecnológicos del **IMSS**, entre los que se mencionan de manera enunciativa mas no limitativa, aplicaciones, servidores, equipos de comunicación, base de datos, con el fin de detectarlos, clasificarlos y tomas decisiones oportunas ante ellos. La infraestructura propuesta deberá de ser nueva, de última generación y dedicada exclusivamente para las necesidades del **IMSS**, y deberá de cumplir con las siguientes especificaciones técnicas mínimas.

Cumplir con al menos las siguientes funcionalidades operativas:

- Capacidad para recolectar datos de todas las aplicaciones o dispositivos que tengan una fuente de eventos necesarios para la organización, siendo esto a través de desarrollo predefinido del fabricante o con desarrollos personalizados ejecutados por el administrador del servicio.

ANEXOS
DIVISION DE CONTRATOS

- Capacidad para almacenar la información tal y como fue recibida del dispositivo o aplicaciones (eventos en crudo) para efectos de auditoria y análisis forense, la solución deberá genera una firma o "checksum" de los eventos recibidos para garantizar la integridad y mantener la cadena de custodia.
- Permitir la detección automática de fuentes de eventos recolectados a través del protocolo syslog, el cual puede ser enviado vía UDP, TCP o SSL/TLS.
- Capacidad de permitir el filtrar eventos por cualquier campo de registro, que son los atributos donde se almacena la información recolectada por la herramienta de las fuentes de eventos.
- Contar con lógica de taxonomía a nivel de recolección de eventos, y que permita definir y modificar la misma con base a los eventos auditados.
- Capacidad para detectar automáticamente la desconexión un conector de integración a través del envío de señales de comunicación para el aseguramiento de la continuidad operativa ("keepalive").
- Capacidad para integrarse con los sistemas de detección y prevención de intrusos y los de administración de vulnerabilidades (VM).
- Contar con la capacidad de emitir notificaciones a partir de eventos y datos recopilados a través de mecanismos como SMTP, SNMP, y SYSLOG.
- Correlacionar eventos en tiempo real, es decir, que la información de los eventos sobre los que se está basando deberá venir del flujo del bus de mensajes.
- Capacidad para definir reglas de correlación con diferentes niveles de complejidad, partiendo de las basadas en patrones, hasta reglas basadas en periodos de tiempo, anidadas, causas/efecto, y secuenciales.
- El módulo de creación de reglas de correlación deberá tener la capacidad de seleccionar eventos para hacer las reglas, así como de seleccionar campos del mismo para ser incluidos en la regla a través de mecanismos como "Drag and Drop".
- Contar con la capacidad de probar las reglas antes de ser implementadas en el motor de correlación.
- Deberá comprimir los datos almacenados al menos con una relación de 10 a 1.
- Contar con mecanismos de monitoreo de la integridad local y archivada.
- Capacidad para soportar de forma nativa la integración con soluciones de almacenamiento en red como SAN, NAS, NFS, o CIFS.
- Contar con una suscripción de boletines de seguridad más importantes del mercado para así identificar las vulnerabilidades conocidas, correlacionando la información de herramientas de administración de vulnerabilidades con los eventos recolectados lo que permitirá automatizar su detección.

13.1.7 Borrado Seguro de Datos.

Realizar el borrado seguro de información en servidores, equipos de centro de datos, discos duros externos, y otras unidades de almacenamiento que imposibilite, ante cualquier intento o medio, la recuperación de la información borrada y permita la generación de un certificado que respalde la ejecución de borrado, esto debe ser totalmente automatizado y gestionado centralmente.

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

- Debe permitir realizar borrados completos en servidores derivados de sustitución de equipos, migraciones tecnológicas, o retiro por finalización de contrato.
- Debe asegurar que los datos no puedan ser recuperados, basándose en al menos los siguientes estándares internacionales:
  - HMG, Infosec Standard 5 (Baseline and Enhanced).
  - OPNAVINS5239.1
  - Extended NIST800-88
  - DoD5220.22-M.

- Borrado de discos duros IDE/ATA, SCSI, SAS, USB, SATA, Fiberchannel, y Firewire de cualquier tamaño.
- Debe brindar la destrucción local y remota en múltiples dispositivos de almacenamiento.
- Debe posibilitar el desmontaje RAID (SCSI).
- Debe permitir el borrado y detección de zonas bloqueadas/ocultas (DCO, HPA).
- Deberá generar certificados de borrado infalsificables que ofrezcan protección ante cualquier instancia legal en donde se incluya el resultado el proceso de borrado, fecha, hora, los datos del equipo, el detalle del HD borrado.
- Deberá emitir una firma electrónica para la autenticación de la integridad del reporte de sanitización emitido por el software de borrado.
- La solución debe poder ejecutarse sin importar de que sistema operativo se trata.
- El reporte que genera la solución deberá poder ser exportado a un medio de almacenamiento como USB o disco duro.

13.1.8 Servicio de Seguridad Perimetral para enlaces de banda ancha.

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

Detalles del Servicio.

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

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

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

- Deberá contar un servicio de IPS.
- Deberá contar con puertos de cobre Rj45
- Deberá ser un dispositivo de nivel empresarial.
- Deberá ser un dispositivo multifuncional, es decir integrar las funcionalidades descritas a continuación:
  - Firewall
  - IPS
  - Filtrado de Contenido
  - Detección y control de amenazas y programas maliciosos.
- Deberá contar con una consola de administración integrada accesible vía remota.
- Deberá contar con doble fuente de poder.
- Deberá garantizar técnicamente la seguridad de datos.
- Deberá ser compatible con direccionamiento IPv4 e IPv6
- Deberá contar con la capacidad de manejo de VLANS.
- Deberá poder operar de manera transparente como un dispositivo de capa 2 y como un dispositivo de capa 3.
- Deberá operar en alta disponibilidad tomado en cuenta los siguientes esquemas:
  - Modo Ruteo en capa 3 Activo/Activo
  - Modo Ruteo en capa 3 Activo/Pasivo
- Deberá incluir la capacidad de generar túneles VPN a través de protocolos IPSEC.
- Deberá poder aplicar QoS (Quality of Service) para priorizar tráfico de datos y/o video.

ANEXOS
DIVISION DE CONTRATOS

- Deberá poder crear políticas para usuarios y para grupos.
- Deberá poder identificar, permitir, bloquear o limitar el uso de aplicaciones independientemente del puerto.
- Deberá permitir el escaneo
- Deberá contar con la administración centralizada de acceso a usuarios, a los recursos del **IMSS** y aplicaciones en Internet.
- Deberá permitir la conexión a las aplicaciones del **IMSS** a través de dispositivos móviles.

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

- Deberá contar un servicio de IPS.
- Deberá contar con puertos de cobre Rj45
- Deberá ser un dispositivo de nivel empresarial.
- Deberá ser un dispositivo multifuncional, es decir integrar las funcionalidades descritas a continuación:
  - Firewall
  - IPS
  - Filtrado de Contenido
  - Detección y control de amenazas y programas maliciosos.
- Deberá contar con una consola de administración integrada accesible vía remota.
- Deberá contar con doble fuente de poder.
- Deberá garantizar técnicamente la seguridad de datos.
- Deberá ser compatible con direccionamiento IPv4 e IPv6
- Deberá contar con la capacidad de manejo de VLANS.
- Deberá poder operar de manera transparente como un dispositivo de capa 2 y como un dispositivo de capa 3.
- Deberá operar en alta disponibilidad tomado en cuenta los siguientes esquemas:
  - Modo Ruteo en capa 3 Activo/Activo
  - Modo Ruteo en capa 3 Activo/Pasivo
- Deberá incluir la capacidad de generar túneles VPN a través de protocolos IPSEC.
- Deberá poder aplicar QoS (Quality of Service) para priorizar tráfico de datos y/o video.
- Deberá poder crear políticas para usuarios y para grupos.
- Deberá poder identificar, permitir, bloquear o limitar el uso de aplicaciones independientemente del puerto.
- Deberá permitir el escaneo
- Deberá contar con la administración centralizada de acceso a usuarios, a los recursos del **IMSS** y aplicaciones en Internet.
- Deberá permitir la conexión a las aplicaciones del **IMSS** a través de dispositivos móviles.

13.1.9 Soporte para la operación de la Seguridad de la Nube IMSS.

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

alertas y vulnerabilidades, así como el establecimiento de acciones de mejoras sustentable. A continuación se detalla el Servicio:

- Ubicarse dentro del territorio mexicano (A fin de que se encuentre dentro de jurisdicción de las leyes mexicanas).
- Contar con un mecanismo que garantice la continuidad de la operación frente a contingencias.
- Operación 7x24x365 días durante la vigencia del contrato.
- Personal en sitio y remoto altamente calificado con las credenciales requeridas para la administración y monitoreo de los componentes que integran la solución.
- Operación de un centro de datos alterno ubicado dentro del territorio nacional.
- 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 de 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.
- Revisiones continuas de la operación del SOC, que permitan establecer mejora en los procesos, procedimientos y controles de seguridad.
- Servicio de correlación de eventos de seguridad y administración de bitácoras.
- Equipo de 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, intermitencia y /o perdida 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 Servicios apegada a ITILv3

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

- Numero directo de las instalaciones del SOC.
- Un numero 01 800 sin costo.
- Correo electrónico.

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

ANEXOS
DIVISION DE CONTRATOS

- Currículum Vitae de todo el personal deberá indicar al menos:
  a. Experiencia profesional: Bajo este rubro se considerarán todos los cargos que cada integrante haya desempeñado.
  b. Experiencia en proyectos de su especialidad.
  c. Estudios: Bajo este rubro se anotarán todos los estudios en materia de seguridad de la información.
  d. Incluir la estructura del grupo de trabajo, indicando por cada perfil la responsabilidades y competencias
  e. El **IMSS** 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.

13.1.10 Administración y Soporte de Componentes de Seguridad.

13.1.10.1 Firewall

El **IMSS** 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 nueva de última generación y dedicada exclusivamente para las necesidades del **IMSS** y deberá cumplir el **LICITANTE** con las siguientes especificaciones mínimas:

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los Firewalls en la arquitectura de seguridad y comunicaciones.
- Habilitar esquema de alta disponibilidad.
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en las zonas del centro de datos correspondiente, o en su caso, donde le sea solicitado por el **IMSS**.
- Acordar con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware y software que integran el servicio sin ningún control de cambios autorizados por este último.
- Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Asegurar que el equipo propuesto cuente con la última versión estable, validad 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 **IMSS**.
- Permitir únicamente el tráfico definido por el **IMSS** 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 **IMSS**.

- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** 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 las 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 este caso de que el desempeño de la tecnología que soporta el servicio deberá realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades.

13.1.10.2 IPS

El **IMSS** 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 pudiera 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 de la **IMSS** y deberá cumplir con las siguientes especificaciones técnicas mínimas:

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los Equipos de Prevención de intrusos (IPS por sus siglas en ingles) en la arquitectura de seguridad y comunicaciones.
- Habilitar esquema de Alta Disponibilidad (HA por sus siglas en ingles).
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el **IMSS**.
- Acordar con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes hardware/software que componen el servicio sin un control de cambios autorizado por este último.
- Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante. Siempre y cuando esté autorizado por el **IMSS**.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** 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 las soluciones de Prevención de Intrusos relacionados para al menos:
  - Cumplir las políticas de reglas de acceso a la Información.
  - Notificación sobre las actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución.
  - Notificar todas aquellas actividades sospechosas que sean las identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el **LICITANTE** del servicio deberá realizar la sustitución de componentes tecnológicos por otros de igual o mejores características/funcionalidades.

ANEXOS
DIVISION DE CONTRATOS

13.1.10.3 Anti-denegación de Servicios (DDoS).

El **IMSS** 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 nueva, de última generación y dedicada exclusivamente para las necesidades del **IMSS** y deberá cumplir con las siguientes especificaciones técnicas mínimas:

- El **LICITANTE** debería definir en conjunto con el **IMSS** la estrategia de habilitación de los equipos de Anti-denegación de Servicios (DDoS) en la arquitectura de seguridad y comunicaciones.
- El **LICITANTE** deberá habilitar esquema de Alta Disponibilidad (HA por sus siglas en ingles).
- El **LICITANTE** deberá llevar a cabo todas las tareas necesarias para la Instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el **IMSS**.
- El **LICITANTE** deberá acordar con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes hardware/software que componen el servicio sin un control autorizado por este último.
- El **LICITANTE** deberá 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.
- El **LICITANTE** deberá asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.
- El **LICITANTE** deberá prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- El **LICITANTE** deberá atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- El **LICITANTE** deberá emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Anti-denegación de Servicios (DDoS) relacionados para al menos:
  - Cumplimiento de las políticas de uso de información implantadas en la solución.
  - Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución.
  - Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el **LICITANTE** deberá realizar solución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

13.1.10.4 Redes Virtuales Privadas (VPN).

El **IMSS** requiere del Servicio de Interconexión a través de Internet que permita establecer comunicación desde localidades remotas para la transferencia de información a través de un canal cifrado.

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los equipos para Redes privadas Virtuales – VPN en la arquitectura de seguridad y comunicaciones.
- Habilitar esquema de Alta Disponibilidad (HA por sus siglas en ingles).

- Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde lo sea solicitado el **IMSS**.
- Acordar con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes hardware/software que componen el servicio sin un control de cambios autorizado por este último.
- Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- Gestionar el alta de accesos remotos debida y previamente autorizados por el **IMSS** a través de los mecanismos y personal que para ellos designe este último.
- Solicitar de manera semanal la lista de usuarios dados de baja por la organización y proceder a la deshabilitación de sus accesos remotos de manera inmediata.
- Reportar bajo demanda la lista de usuarios y entidades (terceros) que cuentan con acceso remoto VPN C2S – S2S.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** 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 las soluciones de Prevención de Intrusos relacionados para al menos:
  - Cumplir las políticas de reglas de acceso a la Información.
  - Notificar sobre las actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución, configuradas para las cuentas de usuario o servicios con terceros.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el **LICITANTE** deberá realizar solución de componentes tecnológicos por otros de igual o mejor características/funcionalidades.

13.1.10.5 Filtrado de Contenido Web.

El **IMSS** requiere del servicio de filtrado de contenido Web mediante políticas de acceso que permita controlar y filtrar la utilización del servicio de acceso a Internet, en función de roles y perfiles. La infraestructura propuesta deberá ser nueva, de última generación y dedicada exclusivamente para las necesidades del **IMSS** y deberá cumplir con las siguientes especificaciones técnicas mínimas:

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los equipos de Filtrado de Contenido Web en la arquitectura de seguridad y comunicaciones.
- Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el **IMSS**.
- Acordar con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último,
- Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante. Siempre y cuando esté autorizado por el **IMSS**.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** genere, apegado a los Niveles de Servicio definidos para dicho propósito.

- Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Filtrado de Contenido de Correo relacionados con al menos:
  - Cumplir las políticas de reglas de acceso a la información.
  - Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución. configuradas para las cuentas de usuario.
  - Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución de Filtrado de Contenido Web, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.
- Acordar con el **IMSS** el tipo de implementación que se integrará para el uso de los servicios (modo implícito o explicito), y en su caso, podrá solicitar modificaciones al uso del mismo conforme las necesidades operativas así lo demanden.

13.1.10.6 Antispam

El **IMSS** requiere del servicio de analizar correos electrónicos de entrada y salida con el objetivo de bloquear amenazas de spam, malware, phishing, amenaza persistente avanzada (Advanced Persistent Threat APT's), reputación de URLs embebidas en los correos. La infraestructura propuesta deberá ser nueva, de última generación y dedicada exclusivamente para las necesidades del **IMSS** y deberá cumplir con las siguientes especificaciones-técnicas mínimas:

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los equipos de Filtrado de Contenido de Correo electrónico (Antispam) en la arquitectura de seguridad y comunicaciones.
- Habilitar esquema de Alta Disponibilidad (HA por sus siglas en ingles).
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el **IMSS**.
- Acordar con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.
- Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante. Siempre y cuando esté autorizado por el **IMSS**.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- Conocer y entender las políticas actuales de seguridad del **IMSS**, particularmente aquellas relacionadas con el manejo de información, las cuales serán entregadas en las Mesas de Trabajo correspondientes por parte del personal del **IMSS**.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Filtrado de contenido de Correo relacionados con al menos:
  - Cumplir las políticas de reglas de acceso a la información.
  - Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución, configuradas para las cuentas de usuario.
  - Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución de Filtrado de Contenido de Correo, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea adecuado, el **LICITANTE** del servicio deberá realizar la sustitución de componentes tecnológicos por otros de igual o mejor caracteristicas/funcionalidad.

13.1.10.7 Antimalware.

El **IMSS** requiere de un servicio de detección y protección contra amenazas avanzadas en la red interna. La infraestructura propuesta deberá ser nueva, de última generación y dedicada exclusivamente para las necesidades del **IMSS** y deberá cumplir con las siguientes especificaciones técnicas mínimas:

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los equipos de Antimalware en la arquitectura de seguridad y comunicaciones.
- Habilitar esquema de Alta Disponibilidad (HA por sus siglas en ingles).
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el **IMSS**.
- Acordar con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.
- Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** genere, apegado a los Niveles de Servicio definidos para dicho propósito.
  - Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Antimalware relacionados para al menos.
  - Cumplimiento de las políticas de uso de información implantadas en la solución.
  - Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habitadas en la solución, configuradas para el tráfico externo y/o interno.
  - Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el **LICITANTE** del servicio deberá realizar la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

13.1.10.8 Firewall Especializado en Servicios Web (WAF).

El **IMSS** requiere del servicio de protección, prevención y control de ataques para aplicativos webs expuestos en Internet. La infraestructura propuesta deberá ser nueva, de última generación y dedicada exclusivamente para las necesidades del **IMSS** y deberá cumplir con las siguientes especificaciones técnicas mínimas:

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los equipos de Firewall Especializado en Servicios Web (WAF) en la arquitectura de seguridad y comunicaciones.
- Habilitar esquema de Alta Disponibilidad (HA por sus siglas en ingles).
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el **IMSS**.
- Acordar con el personal del **IMSS** 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
DIVISION DE CONTRATOS

- Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- Revisar y validar en conjunto con el **IMSS** los requerimientos de protección, inspección de contenido http o https y de seguridad de aplicativos webs tal y como sea solicitado.
- Aprovisionar nuevos servicios aplicativos que requieran la protección a través del WAF, conforme el **IMSS** lo necesite.
- 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 **IMSS** 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 habitadas en la solución, configuradas para los servicios web públicos y/o privados.
  - Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el **LICITANTE** del servicio deberá realizar la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

13.1.10.9 Firewall Especializado de base de datos.

El **IMSS** requiere del servicio de protección a las instancias de base de datos en tiempo real, así como el monitoreo del tráfico de base de datos con la finalidad de realizar la detección de ataques avanzados. La infraestructura propuesta deberá ser nueva, de última generación y dedicada exclusivamente para las necesidades del **IMSS** y deberá cumplir con las siguientes especificaciones técnicas mínimas:

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los equipos de Firewall Especializado en Base de Datos (DBF) en la arquitectura de seguridad y comunicaciones.
- Habilitar esquema de Alta Disponibilidad (HA por sus siglas en ingles).
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el **IMSS**.
- Acordar con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.
- Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.

- El **LICITANTE** deberá atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- El **LICITANTE** deberá emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Firewall Especializado en Base de Datos (DBF) 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 habitadas en la solución, configuradas para los servicios de base de datos privadas.
  - Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el **LICITANTE** del servicio deberá realizar la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

13.2 Servicio de Administración de Riesgos Tecnológicos, (procesos ASI y OPEC)

Apoyar al **IMSS** en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado al MAAGTICSI y basado en el estándar ISO 27001, que permita emitir directivas en materia de seguridad de la información a las áreas de TI y a los terceros que soportan la operación de TI.
El **LICITANTE** del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

- Planear.
- Transferencia tecnológica Inicial – Curso "Inducción a la norma 27001:2013" Curso Introductorio que permite al participante:
  - Conocer la estructura de la norma ISO/IEC 27001:2013.
  - Interpretar los requisitos solicitados para el cumplimiento de la norma.
  - Conocer las etapas para la implementación de un SGSI.
- Generación de Directivas de Seguridad, manual de políticas de seguridad de la información:
  - Basadas en los dominios que establece la norma ISO 27001.
  - Alineados a los procesos de seguridad ASI y OPEC del MAAGTICSI.
  - Enfocadas a las áreas de TI y a los terceros que proveen servicios de TI al **IMSS**, considerando como alcance el catálogo de Infraestructuras Criticas del **IMSS**.
- Identificación y valuación de activos (Relacionado al catálogo de Infraestructuras Criticas) del proceso involucrado en el Sistema de Seguridad de la Información. La metodología contempla los siguientes puntos:
  - Identificación de los activos del proceso.
  - Valoración de los activos del proceso.
  - Identificación de requerimientos de seguridad.
  - Identificación de los controles de seguridad existentes.
- Generación de la Declaración de Aplicabilidad (SoA). La metodología contempla los siguientes puntos:
  - Identificación y aplicabilidad de los requerimientos internos y externos.
  - Selección de los objetivos control y controles para el tratamiento de los riesgos
  - Verificación de requerimientos contractuales y legales.
  - Identificación de los requerimientos internos y externos.
  - Validación de aplicabilidad de los requerimientos.

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

- Análisis de Riesgos de Seguridad de la Información.
- Realización del Análisis de Riesgo con base en lo definido en el Servicio de Gestión de Riesgos de Seguridad.
- Generación del Plan de Tratamiento de Riesgos. La metodología contempla los siguientes puntos:
  - Identificación de las acciones a realizar por parte de la Organización y su Administración.
  - Identificación de los recursos necesarios y prioridades.
  - Identificación de las responsabilidades para administrar los Riesgos de Seguridad de la Información.
- Aplicación del Plan de Tratamiento de Riesgos. La metodología contempla los siguientes puntos:
  - Asignación de los roles y responsabilidades en la implantación de los controles relativos apersonas, procesos y tecnología involucrados en la mitigación de los riegos.
  - Actualización de documentación. Alineada a los requisitos establecidos en el proceso ASI y OPEC de MAAGTICSI.
  - Afinación de políticas y procedimientos de seguridad existentes.
  - Definición del proceso de reporte y atención de incidentes de seguridad (ERISC).
- Propuestas de implementación de los controles seleccionados, la metodología contempla los siguientes puntos:
  - Control de Accesos.
  - Monitoreo de Cuentas.
  - Definición del proceso de continuidad del negocio.
  - Implantación de los roles y responsabilidades definidas para el Sistema de Gestión de Seguridad de la Información.
  - Controles de Seguridad en la Infraestructura Tecnológica de acuerdo a lo definido en el alcance.
- Administración del cambio cultural. La metodología contempla los siguientes puntos:
  - Desarrollo de un programa de concientización con usuarios y operadores s del Sistema de Gestión de Seguridad de la Información.
  - Determinación de las necesidades de Transferencia tecnológica para el personal que administre el Sistema de Gestión de Seguridad de la Información.
  - Apoyo en la Transferencia tecnológica relativa a temas de seguridad de la información.
  - Manual de Gestión de Seguridad de la Información. Se documentará un manual que contiene las referencias de la documentación generada en esta fase para dar trazabilidad al de las cláusulas de la norma.
  - Monitorear y Revisar el Sistema de Gestión de Seguridad la Información.
- Revisiones gerenciales. La metodología contempla los siguientes puntos:
  - Los dueños de procesos deben hacer una revisión al sistema de gestión de seguridad la información a fin de verificar que los objetivos del Sistema de Gestión de Seguridad de la Información están alineados a los objetivos de negocio en materia de seguridad de la información y que garantizan el adecuado manejo de los riesgos existentes.
  - El **LICITANTE** generara el procedimiento de revisiones Gerenciales.
  - El **LICITANTE** propondrá los formatos requeridos para llevar acabo las revisiones.

Auditorías Internas La metodología contempla lo siguiente:

- Apoyo en la generación del plan de auditorías internas a las áreas de TI y los terceros que proveen servicios de TI al **IMSS**.
- Definición de los formatos requeridos para llevar a cabo las auditorias.
- Aplicación de una auditoría interna al Sistema de Gestión de Seguridad de la Información para verificar el cumplimiento con el estándar ISO/IEC 27001:2013 y a los procesos de seguridad ASI y OPEC del MAAGTICSI.
- Mantener y mejorar el Sistema de Gestión de Seguridad de la Información

- Implementación de mejoras. Contempla los siguientes puntos:
  - Priorización de las acciones correctivas y no conformidades identificadas en las revisiones gerenciales, revisiones independientes, auditorías internas y revisiones técnicas.
  - Identificación de los responsables de llevar a cabo las mejoras por parte de la organización.
  - El **IMSS** definirá las fechas compromiso para la terminación de las mejoras, únicamente para el seguimiento interno.
- Tomar acciones correctivas y en las no conformidades. Contempla los siguientes puntos:
  - Apoyo en la definición del procedimiento para realizar acciones correctivas y no conformidades derivadas de las auditorías.
  - Definición del formato para el llenado de acciones correctivas y no conformidades.
  - Coordinación de la ejecución de las acciones correctivas ya definidas y en su caso las no conformidades que se identifiquen.
- Comunicar los resultados de las acciones tomadas. Contemplar el siguiente punto:
  - Apoyo en la programación de reuniones de seguimiento al Sistema de Gestión de Seguridad de la Información para dar a conocer el alcance de las acciones correctivas y no conformidades realizadas y verificar su apego a los requerimientos de los dueños de la información y los involucrados en los procesos del **IMSS**
  -

13.3 Servicio de Análisis de riesgos (procesos ASI y OPEC), apéndice seguridad

Identificar, evaluar y manejar los riesgos de la seguridad de la información, utilizando técnicas estadísticas, información histórica, fuentes de información especializada y otras que permitan, determinar la exposición a diferentes escenarios de riesgo, probabilidad e impacto, así como la recomendaciones y líneas de acción, que permita alcanzar un nivel de seguridad aceptable a un costo razonable enfocado al catálogo de infraestructura críticas del **IMSS**. El **LICITANTE** del servicio deberá de cumplir con las siguientes funcionalidades operativas:

- Contexto
  - Recopilar información sobre las operaciones del **IMSS**, las relaciones entre los procesos de negocio, procesos y recursos de tecnológica, las dependencias entre estos, tomando en cuenta:
    a. Consideraciones generales del **IMSS**.
    b. Definición de criterios básicos para la ejecución del análisis.
    c. Definición del alcance del análisis.
    d. Definición del equipo de trabajo del **LICITANTE** y del **IMSS** que participara en la ejecución del análisis.
- Valoración de Riesgos
  - Utilizar la metodología basada en el proceso ASI del MAAGTICSI para la gestión de riesgos de la seguridad. La metodología contendrá:
    a. Identificación de activos, considerando como activos a los procesos, actividades, información, infraestructura, y gente.
    b. Identificación de vulnerabilidades.
    c. Identificación de amenazas.

d. Escenarios de riesgo.
e. Priorización del riesgo.

- Tratamiento de los riesgos.
  - Criterios para la atención del riesgo identificado y analizando varias opciones de tratamiento de las cuales se elegirá la que mejor balance Costo-Beneficio genere, considerando el resultado obtenido:
    a. Evitar
    b. Mitigar
    c. Transferir
    d. Aceptar
- Seguimiento y Mitigación de Riesgos.
  - Deberá dar seguimiento a los planes de tratamiento de riesgos conforme a lo siguiente:
    a. La generación de los planes de mitigación de riesgos.
    b. Identificación de los responsables de cada plan.
    c. Acompañamiento en la implementación de controles normativos.

13.4 Entregables de única ocasión.

Centro de Operaciones de Seguridad (SOC).

- Diseño físico y lógico de alto nivel con la descripción detallada de la arquitectura propuesta para habilitar los servicios de la solución de seguridad.
- Copia de los siguientes procesos de seguridad que tiene implementados en el "SOC":
  - Proceso de Administración y Control de Cambios.
  - Proceso de Disponibilidad.
  - Proceso de Administración de Vulnerabilidades.
  - Proceso de Atención y Respuesta a Incidentes.
  - Proceso de Mejora Continua.
- La matriz de escalamiento del servicio tanto técnico como jerárquica.
- Procesos de la Mesa de Servicio, que se indican a continuación:
  - Administración de incidentes.
  - Administración de problemas.
  - Administración de cambios y configuraciones.
  - Administración de liberaciones.
- Metodología para el proceso de administración de vulnerabilidades.
- Procedimientos de seguridad aplicados en el "SOC" para:
  - Manejo de alarmas.
  - Análisis y Correlación de Eventos de Segundad.
  - Atención y Respuesta a Incidentes de Seguridad.

13.5 Entregables periódicos.

El **LICITANTE** deberá generar de manera integrada un Entregable Mensual del Servicio de Seguridad, que incluya de manera enunciativa más no limitativa los siguientes conceptos:

13.5.1 Firewall.

- Reporte de la disponibilidad de los activos de infraestructura (firewall), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (firewall), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (firewall), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (firewall), incluyendo tiempos de solución.
- Reporte de promedio de tráfico de entrada/salida por cada DMZ asignada.
- Reporte del top diez (10) de los protocolos bloqueados.
- Reporte del top diez (10) de los protocolos permitidos.
- Repone de reglas de control de acceso más utilizadas.
- Reporte del top diez (10) de direcciones IP Publicas/Privadas con más consumo de ancho de banda.

13.5.2 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.

13.5.3 Anti-denegación de Servicios (DDoS).

- Reporte de la disponibilidad de los activos de infraestructura (AntiDDoS), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (AntiDDoS), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (AntiDDoS), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (AntiDDoS), incluyendo tiempos de solución.
- Reporte del top diez (10) de anomalías clasificadas por nivel de severidad.
- Reporte del top diez (10) de activos de infraestructura con mayor número de incidencias de tráfico anómalo (internos/externos).
- Reporte del top diez (10) de protocolos bloqueados.

13.5.4 Redes Privadas Virtuales – VPN.

- Reporte de la disponibilidad de los activos de infraestructura (Concentrador VPN), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (Concentrado VPN), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (Concentrador VPN), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (Concentrador VPN), incluyendo tiempos de solución.
- Reporte del top diez (10) usuarios que se conectan a través de VPN C2S.
- Reporte del top diez (10) de servicios (direcciones 1P destino) que se conectan a través de VPN C2S y S2S.
- Reporte del top diez (10) de ancho de banda consumido por VPN S2S.

13.5.5 Filtrado de Contenido Web.

- Reporte de la disponibilidad de los activos de infraestructura (Filtrado de Contenido Web), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (Filtrado de Contenido Web), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (Filtrado de Contenido Web), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (Filtrado de Contenido Web), incluyendo tiempos de solución.

- Reporte del top veinte (20) sitios web bloqueados.
- Reporte del top veinte (20) sitios web permitidos.
- Reporte del top veinte (20) categorías bloqueadas.
- Reporte del top veinte (20) categorías permitidas.
- Reporte del top veinte (20) de IP/Usuarios con mayor navegación a Internet,
- Reporte del top veinte (20) de IP/Usuarios con mayor consumo de ancho de banda.

13.5.6 Antispam.

- Reporte de la disponibilidad de los activos de infraestructura (Antispam), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de Infraestructura (Antispam), incluyendo tiempo de atención.

13.6 Entregables bajo demanda.

El **LICITANTE** generara bajo demanda los siguientes documentos y/o reportes, a solicitud del órgano de gobierno que señale el **IMSS**; y que incluyen de manera enunciativa más no limitativa los siguientes conceptos:

13.6.1 Servicios de Control de Calidad.

13.6.1.1 Análisis de Vulnerabilidades

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades, detectadas por cada activo o grupo de activos de infraestructura Escaneados, así como el plan de mitigación propuesto.
- Archivos electrónicos (MS Excel) con la información fuente obtenida de las herramientas tecnológicas que se utilizaron para realizar los escaneos de vulnerabilidades.
- Reporte de los escaneos de vulnerabilidades realizados, indicando al menos: Activo(s) De infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja).

13.6.1.2 Pruebas de Penetración.

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades, detectadas por cada activo o grupo de activos de infraestructura Verificados, así como el plan de mitigación propuesto.
- Archivos electrónicos (MS Excel) con la información fuente obtenida de las herramientas tecnológicas que se utilizaron para realizar las pruebas de penetración.
- Reporte de las pruebas de penetración realizadas, indicando al menos: Activo(s) De infraestructura o aplicativo relacionado, fecha de ejecución, direccionamiento IP, Vulnerabilidades detectadas (Alta, Media, Baja).

13.6.1.3 Análisis Forenses.

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle del análisis forense ejecutado por cada activo o grupo de activos de infraestructura verificados.

13.6.1.4 Borrado Seguro de Datos.

ANEXOS
DIVISION DE CONTRATOS

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro por cada activo o grupo de activos de infraestructura eliminados.
- Archivos electrónicos (HTML y PDF) con la información fuente obtenida de las herramientas tecnológicas que se utilizaron para realizar los borrados seguros de la información.
- Reporte mensual de los borrados seguros realizados, indicando al menos: Activo(s) de infraestructura, fecha de eliminación.

13.6.1.5 Análisis de Riesgos de Seguridad de la información.

- Reporte ejecutivo en formato electrónico (MS Word, PDF) de la actividad de Análisis de Riesgos que incluya:
  - Identificación activos, considerando como activos a los procesos, actividades, información, infraestructura, y gente.
  - Identificación de vulnerabilidades.
  - Identificación de amenazas.
  - Escenarios de riesgo.
  - Priorización del riesgo.

13.6.1.6 Sistema de Gestión de Seguridad de la Información (SGSI).

- Reporte de actividades relacionadas con las solicitudes de implementación, Evaluación y/o Mejora del sistema de Gestión de Seguridad de la Información que incluya:

  - Transferencia tecnológica inicial
  - Generación de directivas de seguridad
  - Identificación y valuación de activos
  - Generación de la Declaración de Aplicabilidad
  - Generación del plan de tratamiento de riesgos
  - Propuestas de implementación de los controles
  - Manual de Gestión de seguridad de la información

Los reportes y/o documentos anteriores deberán ser entregados en el formato y fecha que hayan sido acordados con el órgano de gobierno del **IMSS** que los haya solicitado y deberán ser integrados al Entregable Mensual del servicio de Seguridad) en el periodo que corresponda a su entrega, para la validación de los niveles de servicio que correspondan.

13.7 Consideraciones generales para la entrega de los servicios de seguridad.

El **LICITANTE** deberá fortalecer la seguridad de la información de la Institución contra amenazas, disminuyendo el riesgo de sufrir incidentes de seguridad, mediante el uso de tecnología de punta para el monitoreo, detección, aseguramiento, y contención de ataques que puedan presentarse en la infraestructura de cómputo, sistemas y aplicaciones del **IMSS**.

- Contar con servicios de infraestructura regulados por niveles de servicio, que: implementen (instalen, migren, habiliten y pongan a punto) los componentes necesarios en los Centros de Datos del **IMSS**, 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 optimas 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 **IMSS**.
- 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 **IMSS**, entendiendo que toda actualización o mejora debe ser consultada y aprobada por este último.
- Garantizar la operación. Licenciamiento, soporte técnico, mantenimiento correctivo y preventivo, así como el reemplazo de partes (por parte del fabricante del componente o de la solución), de los servicios propuestos, considerando la cantidad de unidades de licenciamiento como los dispositivos, los usuarios concurrentes. entre otros, conforme la naturaleza y características del servicio que dicha infraestructura y base instalada soportan.
- Integrar a los servicios de gestión, operación, soporte y mantenimiento provistos por su Centro de Operaciones de Seguridad (SOC) para los servicios ofrecidos, dando cumplimiento a las condiciones del presente contrato.
- Establecer Mesas de trabajo con el **IMSS**, 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 **IMSS** 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 un número telefónico 01 800 para dar soporte a los usuarios del **IMSS**.
- 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 **IMSS** validar en cualquier momento los elementos que componen los diversos servicios.

14 TRANSFERENCIA DE CONOCIMIENTO Y ADIESTRAMIENTO TÉCNICO

El **LICITANTE** deberá establecer un plan para la transferencia de conocimiento y adiestramiento técnico en las diferentes herramientas, tecnologías de la información y/o componentes con las cuales se bridará el servicio, impartiendo y transfiriendo el conocimiento al personal técnico definido por el **IMSS**, todo esto para al menos 15 personas por tema, y entregando en su propuesta el listado de temas, nombre, número o identificador de curso por tecnología propuesta, así como la duración en horas de cada uno de estos.
La transferencia de conocimiento y adiestramiento técnico, deberá ser, preferentemente en español o en su caso, en idioma inglés, con un enfoque a los componentes de la plataforma virtualizada que integran el servicio.

Con el objetivo de no frenar el avance del proyecto, la etapa de transferencia de conocimiento se establecerá con el **LICITANTE** de forma posterior a la implementación y estabilización de los servicios, coordinando y estableciendo fechas y sedes.

Los cursos podrán ser teóricos y/o teórico-prácticos y podrán ser impartidos en las instalaciones del **IMSS** en la Ciudad de México o de acordarse con el **IMSS** de forma remota, según sea más conveniente.
El **LICITANTE** deberá proporcionar los contenidos o materiales informativos de la transferencia de conocimientos a abordar a cada uno de los participantes, ya sea que el expositor sea personal directo del fabricante o bien, una persona certificada.

14.1 Transferencia de conocimiento Tecnológico en plataformas de Código Abierto (virtualización, contenedores, servidores Web, servidores de aplicación, sistemas operativos, bases de datos, etc., ejemplo: Red Hat o equivalente)

El LICITANTE deberá incluir los temarios para la ejecución de la transferencia de conocimiento, los cuales serán analizados, modificados o en su caso aceptados por parte del Instituto en las mesas de trabajo al inicio del contrato. Los temas a considerar deberán estar relacionados con la virtualización, contenedores, servidores web y de aplicación, sistemas operativos, bases de datos u otros que pudiesen existir dentro de la solución propuesta o sujetos a consideración del Instituto.

14.2 Transferencia de conocimiento en Seguridad

El **LICITANTE** deberá implementar y proporcionar la integración de temas que puedan estar relacionados a los servicios que se enlistan a continuación:

- Servicio de Firewalls de siguiente generación
- Servicio de Firewalls perimetrales del tipo A
- Servicio de Firewalls perimetral de tipo B
- Servicio de Firewalls perimetral del tipo C
- Servicio de protección contra ataques DDoS
- Servicio de redes virtuales privadas
- Servicio de Antispam
- Servicio de filtrado WEB
- Servicio de Firewall de aplicaciones web
- Servicio de Firewall de bases de datos
- Servicio de balanceador de carga de capas L4 – L7

15 REPOSITORIOS

15.1 Repositorio Documental

El **LICITANTE** proporcionará mediante el establecimiento de una plataforma (repositorio) los documentos probatorios del servicio, como lo pueden ser entregables, informes, reportes, entre otros, o en su caso, el Instituto definirá el repositorio correspondiente. La plataforma que servirá de contenedor oficial será administrada y soportada por el **LICITANTE.**
La plataforma (repositorio) contará con accesos controlados y definidos por el Instituto, para asegurar la confidencialidad de los documentos que ahí se resguarden, manejando bitácoras de actividad, accesos a documentos, entre otras estadísticas, debiendo entregar cuando menos 3 copias en medio electrónico, al

Instituto al término del contrato, independientemente de la entrega que deberá realizar al proveedor que vaya a dar continuidad a este servicio al término del contrato.

15.2 Repositorio de imágenes de contenedores

El **LICITANTE** deberá proporcionar el espacio en una plataforma de acceso compartido, donde se resguardará el software utilizado durante la operación del proyecto.

La plataforma que servirá de contenedor será administrada, operada y soportada por el **LICITANTE** siendo asignado espacio de la infraestructura asignada para los servicios.

La plataforma (repositorio) contará con accesos controlados y definidos por el Instituto, para asegurar la confidencialidad de la información que ahí se resguarden, manejando bitácoras de actividad, accesos a documentos, entre otras estadísticas.

15.3 Base de conocimientos técnicos de respuesta rápida para publicación de soluciones rápidas (construcción de una base de conocimientos)

El **LICITANTE** deberá realizar las actividades técnicas necesarias para gestionar el conocimiento operativo relacionado a la ejecución de los procesos de soporte, operación y pruebas de la migración; así como con los sistemas informáticos que los sustentan; para que dicho conocimiento sea creado, capturado, transformado y utilizado para brindar visibilidad sobre la operación y los resultados de las pruebas de migración y buscar e identificar áreas de oportunidad para mejorar y sustentar la toma de decisiones respecto a su modelos operativo, etapa de pruebas y migración.

El **LICITANTE** deberá planificar, proveer e implantar, las herramientas tecnológicas necesarias para sustentar el ciclo de vida de dicho conocimiento; así como definir y diseñar los modelos ontológicos y taxonómicos para representar y clasificar el conocimiento tomando en consideración de los modelos establecidos por el propio **IMSS**. Para tales propósitos, se deberán incluir por lo menos los siguientes activos:

- Iniciativas
- Información del contrato o contratos relacionados y acuerdos de trabajo
- Productos y artefactos
- Minutas y evidencias de trabajo y colaboración
- Reportes de incidentes
- Reportes de problemas
- Tableros de indicadores de operación
- Base de datos de gestión de configuraciones (CMDB)

La información anterior es de manera enunciativa más no limitativa y podrán incluirse tópicos según se defina en las mesas de planeación de arranque del contrato.
Estos servicios soportan el modelo de control del contrato del servicio, a través de la integración y revisión de los reportes y demás documentos que formalizan los entregables que soporten el pago de los servicios que valide el Administrador del Contrato.

15.4 CMBD de infraestructura tecnológica.

El **LICITANTE** deberá realizar las acciones necesarias para el diseño, planeación, habilitación, configuración, implementación, operación, gestión, soporte y actualización de la CMBD, en infraestructura

habilitada por el LICITANTE y accesible tanto a personal del LICITANTE como del INSTITUTO de las Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI) y/o de la Coordinación de Ingeniería Tecnológica (CIT).

El **LICITANTE** deberá ejecutar las actividades y un plan para la carga inicial y periódica de los Elementos de Configuración (CIs) de la infraestructura tecnológica física y virtual relacionada al servicio.

El **LICITANTE** deberá entregar de manera mensual un reporte que muestre las altas, bajas o modificación de los elementos de configuración (CIs) durante el periodo.

El LICITANTE expondrá a través de la Intranet del IMSS, la CMDB a manera de blog para consulta únicamente al personal que el Instituto designe.

16 SOPORTE, OPERACIÓN Y MONITOREO DE COMPONENTES LÓGICOS DURANTE LA FASE DE PRUEBAS PARA LA MIGRACIÓN (PLANEACIÓN Y ANÁLISIS DE SOPORTE A SISTEMAS Y SERVICIOS OPERATIVOS)

16.1 Especificaciones para todas las soluciones.

El **LICITANTE** deberá ejecutar las acciones que permitan mantener la continuidad operativa de los servicios lógicos ofertados, desde el suministro, instalación, configuración, puesta a punto e interconexión al ecosistema tecnológico institucional de todas las plataformas requeridas y garantizar la integridad y disponibilidad de los servicios que se describen en el presente anexo.

El **LICITANTE** deberá monitorear el estado de los equipos e infraestructura lógica que integran todos los servicios de tal manera que se generen acciones proactivas para corregir fallas o desviaciones en el desempeño o los niveles de servicio sobre los servicios ofertados. Por lo que el **LICITANTE** deberá considerar todos los componentes y aditamentos necesarios para su diseño, implementación, puesta en marcha y operación de una solución de monitoreo de las plataformas de virtualización y su contenido, que permita la visibilidad de los indicadores de desempeño y salud de la infraestructura virtual y su contenido, además de mostrar indicadores de negocio definidos en conjunto con el Instituto.

El **LICITANTE** deberá incluir personal certificado por la tecnología propuesta a implementarse con el objeto de cumplir todos los requerimientos descritos en el presente anexo, desde la planeación, diseño, implementación, puesta en marcha y operación.

El **LICITANTE** deberá de considerar todas las actualizaciones (updates y demás elementos en software sobre el mismo release o en release diferente) que realice el fabricante con respecto de los bienes objeto del presente documento y en su caso deberá de llevar a cabo la actualización en un ambiente controlado y acordar conjuntamente con el Instituto la instalación en producción sin impacto en los niveles de servicio.

El **LICITANTE** deberá incluir todo el licenciamiento relacionado al equipamiento propuesto de hardware, software y comunicaciones, requeridos para el cumplimiento de funcionalidades y adecuada operación de todos los componentes que integran la plataforma de monitoreo.

El **LICITANTE** deberá contar con un Centro de Atención permanente las 24 horas durante la vigencia del contrato, debiendo proporcionar el soporte de acuerdo a los tiempos de respuesta establecidos en la sección de niveles de servicio.

El **LICITANTE** deberá incluir al recurso humano calificado necesario para la implementación de los servicios de aprovisionamiento virtual y pruebas para la migración.

17 SOPORTE, OPERACIÓN Y MONITOREO DE SERVICIOS DIGITALES ASÍ COMO SUS COMPONENTES LÓGICOS SOBRE LAS PATAFORMAS DE CÓDIGO ABIERTO

El **LICITANTE** deberá contemplar los requerimientos necesarios para brindar el soporte a los componentes principales de las capas de aplicaciones.

El **LICITANTE** contemplará la segregación de las aplicaciones en base a su complejidad, área de negocio, criticidad y afectación en el periodo estacional, haciendo un criterio de asignación de soporte en base a niveles de experiencia de usuarios, siendo dividas en:

- 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 contiene múltiples elementos a migrar dentro de sus capas tecnológicas.
- Mediano; Aplicaciones que dentro de su proceso de migración involucran la migración de datos y que son consideradas aplicaciones críticas dentro del **IMSS**. 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 **IMSS**.

El **IMSS** dentro de lo solicitado como soporte comprende las siguientes categorías con sus diversas aplicaciones actuales susceptibles a las pruebas de migración y en su caso las aplicaciones que sean actualizadas acorde al marco tecnológico de referencia del Instituto, mismo que se definirá en las mesas de arranque del contrato, los siguientes elementos se muestran de manera enunciativa más no limitativa son:

- Gestión de recursos
  - Gestión de identidades
    a. Open AM
    b. Oracle IDM
    c. NetIQ Access Manager Appliance (Access Gateway)
  - Gestión de Infraestructura
    a. Red Hat Cloudforms
    b. Nodos Ansible
- Análisis, reporteo y estadísticas
  - Reportes a la medida (Ad-hoc)
    a. Microsoft Reporting Services
    b. ESSBase
    c. Hyperion
- Inteligencia de negocio
  - Visualización y Análisis de Información
  - Oracle Business Intelligence
  - Microsoft Analisys Services
  - SAS
  - Oracle Exalytics In-Memory Machine
  - Soporte a la toma de decisiones
- Soporte a la toma de decisiones

- Tableau Server
- Tableau Desktop

- Análisis estadístico
  - Stata
- Gestión de datos
  - Extracción, transformación y carga de datos (ETL)
    a. Oracle ODI
    b. IBM Data Stage
    c. Microsoft Integration Services
    d. Oracle Warehouse Builder
    e. Integración y Transformación de Información
    f. Redbrick
    g. Stata Transfer
  - Integración e intercambio de datos
    a. Oracle Golden Gate
  - Gestión de la calidad de los datos
    a. Oracle Data Quality
  - Sistema de gestión de bases de datos
    a. Bases de Datos Oracle
    b. Microsoft SQL Serve
    c. DB2
    d. Subscripciones a Bases de Datos Open Source
    e. Oracle Exadata Storage Expansion
    f. SQL Server Parallel Data Warehouse
  - Directorio
    a. Open DJ
    b. NetIQ Access Manager (Identity Provider)
    c. Plataforma LDAP
    d. Herramientas y entorno de desarrollo
    e. Entorno de desarrollo integrado (IDE)
    f. Team Foundation Server
  - Kit de Desarrollo de Software (SDK)
    a. Java Development Kit
    b. Java Enterprise Edition
    c. Java Runtime Environment
    d. .NET Framework
  - Gestión de documentos y contenidos
    a. Gestión de contenidos Web
       ✓ Drupal
       ✓ Liferay Enterprise
       ✓ Adobe ColdFusion
  - Middleware
    a. Bus de servicios empresariales (ESB)
       ✓ Oracle Service Bus
       ✓ Oracle ALSB
       ✓ Oracle ALDS
       ✓ Red Hat JBOSS Fuse
       ✓ SOA Suite
  - Software de mensajería

  - a. Apache Kafka
- Interfaz o descripción de servicios
  - a. Oracle Enterprise Repository
  - b. Oracle Service Registry
  - c. Red Hat JBoss SOA Enterprise
- Servidores de Aplicaciones
  - a. WebLogic
  - b. Tuxedo
  - c. GlassFish
  - d. Red Hat JBOSS Enterprise Application
  - e. Apache Tomcat
  - f. Apache HTTPD
  - g. Oracle Exalogic
- Automatización y gestión de procesos
  - a. Gestión de procesos de negocios (BPMS)
    - ✓ Oracle BPM
    - ✓ Red Hat JBOSS BPM Suite
- Gestión de reglas de negocio
  - a. Motor de Reglas
- Comunicación unificada y colaboración
  - a. Correo electrónico
    - ✓ Servicio de correo electrónico

Para brindar y garantizar el soporte a las aplicaciones, el **LICITANTE** contemplará perfiles técnicos calificados, certificados y con grados de experiencia acorde a las complejidades de los ambientes, componentes, servicios y aplicativos del Instituto.

18 DISEÑO Y PRUEBAS DE UN PLAN DE RECUPERACIÓN DE DESASTRES Y UN PLAN DE CONTINUIDAD DEL NEGOCIO PARA EL IMSS.

El **LICITANTE** deberá estar situado en un lugar con bajo riesgo o vulnerabilidad ante fenómenos de origen geológico o naturales como pueden ser: sismos, tsunamis o maremotos, vulcanismos, entre otros.

- El **LICITANTE** deberá desarrollar e implementar la metodología para lograr una recuperación de las operaciones y funciones esenciales o críticas del Instituto, en caso de desastres o contingencias.

- El **LICITANTE** deberá elaborar y entregar un plan de trabajo para la generación del "Plan de Recuperación ante Desastres o Contingencias" (DRP), considerando entre otros:
  - Criterios de notificación y escalación para la declaración de un desastre o contingencia y activar los procesos de recuperación,
  - La definición de las estrategias de respaldo y de recuperación de sistemas e infraestructura esencial o crítica, física y/o lógica de recuperación de los sistemas centralizados y descentralizados
  - El plan de retorno y, pruebas del plan y su respectivo mantenimiento y actualización.

- El DRP será documentado con base en un mínimo de 5, a un máximo de 10 escenarios de desastre.

- El **LICITANTE** realizará una prueba de escritorio y posterior a ésta, realizará una prueba en vivo, siempre y cuando El **LICITANTE** y el Instituto cuenten con los elementos necesarios y haya sido

ANEXOS
DIVISION DE CONTRATOS

establecida la planificación de la prueba, se deberán elegir el o los escenarios de desastre o de la contingencia, las estrategias de respaldo y de recuperación, y llevar a cabo la documentación de los resultados de ésta y de los hallazgos identificados durante su ejecución. El alcance de la prueba será definido previo a su ejecución, considerando como mínimo un proceso esencial o crítico y como máximo el total de los procesos críticos definidos por el Instituto.

- Para el desarrollo del "Plan de Recuperación ante Desastres o Contingencias" (DRP), El **LICITANTE**, deberá incluir la identificación de los activos de información necesarios y ubicados en los centros de datos del Instituto y en instalaciones de sus proveedores de centro de datos, que permitan soportar la solución de recuperación definida, con la adecuada coordinación de los equipos encargados de la continuidad operativa y que no estén bajo responsabilidad del **LICITANTE**, además El LICITANTE será responsable de dar soporte durante las pruebas, asignando los recursos humanos idóneos en cantidad y competencias profesionales.

- El **LICITANTE** deberá elaborar y entregar el documento de nombre "Plan de Continuidad de Negocio" (BCP); este plan deberá incluir la documentación necesaria para trabajar de forma manual, de forma electrónica y en papel, la definición de procedimientos alternos, flujos de comunicación identificando los roles y responsabilidades del personal crítico, los recursos físicos y tecnológicos mínimos necesarios, así como la verificación de sitios alternos internos y/o externos.

- El **LICITANTE** deberá incluir en su metodología a implementar las siguientes actividades: Análisis de Riesgos, Análisis de Impacto al Negocio, Planeación de la Continuidad de Negocio y de recuperación, considerando, además las estrategias de respaldo y de recuperación de sistemas e infraestructura, física y virtualizada, de los sistemas centralizados y descentralizados y por último las pruebas de los planes y su respectivo mantenimiento.

- Recomendar diferentes alternativas tecnológicas para instrumentar la capacidad de recuperación en caso de desastre, conforme a la definición y metodología propuesta por el **LICITANTE** y aprobada por el **IMSS** para el Desarrollo del Plan de Recuperación de Desastres (DRP) y del Plan de Continuidad del Negocio (BCP) del **IMSS**.

19 ESPECIFICACIONES TÉCNICAS

Componente o Servicio	Descripción	Especificación	Tipo
Servicios de operación	Establecen las especificaciones, calendarios, niveles de servicio, arquitecturas y lineamientos técnicos para la contratación de los servicios necesarios para la operación de la infraestructura lógica	Gestión de servicios de Tecnologías de la Información	Funcional

20 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. Asimismo, el proveedor 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 en la administración, instalación, puesta a punto, operación, soporte, así como en todas las acciones de gestiones necesarias para brindar el servicio **"Servicio de Soporte Técnico y Operación de la Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube de IMSS y DRP"** que permitan proveer al instituto las capacidades operativas relacionadas a las plataformas de virtualización para el aprovisionamiento de máquinas virtuales de procesamiento, almacenamiento, comunicaciones y seguridad del centro de datos para la Nube Hibrida IMSS, así como todo el soporte necesario para su correcto funcionamiento y las acciones de validación en todos los componentes de infraestructura.

Certificaciones enunciativas más no limitativas en:

CCIE Seguridad
CCIE Routing and Switching
CCIE Service Provider
CCNP Colaboración
CCDP Diseño Profesional de redes.
CCNA Cyber Ops
ITIL Foundation Certificate in IT Service Management
Symantec Data Loss Prevention Prevention 14.5
Symantec Messaging Gateway
APDS - Avaya Networking Solutions
APSS - Avaya Networking Solutions
ISO/IEC 27001
ISO/IEC 20000
ITIL intermediate in Service Design
ITIL intermediate in Operational support and analysis
ITIL intermediate in Service Offering AND Agreements
ITIL intermediate un Release, control and validación.
PCNSE Network Security Engineer 7
MCITP Enterprise Administrator on Windows Server 2008
MCTS Microsoft Exchange Server 2007 Configuration
Extreme Networks Design Specialist - Campus Fabric
Enterasys Certified Specialist – Routing
Enterasys Certified Specialist – Policy.
Security Competency – Technical Accreditation (SCT)
Network Automation Competency – Technical Accreditation (NCT)

ANEXOS
DIVISION DE CONTRATOS

Core Network Services Competency - Technical Accreditation (CNT)
Certificación ITIL RCV, 2017
Certificación ITIL SO, 2016
Certificación ITIL SOA, 2016
Certificación ITIL OSA, 2012
PMI

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

El **LICITANTE** deberá presentar al Instituto, a través de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional cita en Av. Paseo de la Reforma No. 476, Anexo de Telecomunicaciones, Planta Alta, Col. Juárez, C.P. 06600, Ciudad de México, en un plazo no mayor a 5 (cinco) días hábiles posteriores a la adjudicación del contrato, al personal responsable del proyecto; en caso que no se presente el personal en el plazo marcado, se aplicará la pena correspondiente.

El **LICITANTE** deberá presentar en un plazo no mayor a 15 (quince) días hábiles posteriores a la adjudicación del contrato, un plan de trabajo general, para llevar a cabo la implementación del proyecto, en el que se especifiquen las actividades a realizar, la secuencia, los recursos asignados y responsables de dichas actividades, así como la duración del proyecto, su fecha de inicio y de conclusión marcando las fechas de entregables como son cantidad de servicios a entregar de forma única, mensual o eventual.

El **LICITANTE** deberá entregar en un plazo no mayor a 15 (quince) días hábiles posteriores a la adjudicación del contrato, una matriz de escalación con el personal que gestionará los servicios de TIC y con los que el Instituto estará colaborando, su cargo y puesto así como los datos y la vía de comunicación para contactarlo.

21 CONDICIONES TÉCNICAS DE ACEPTACIÓN DE ENTREGABLES

A continuación se relacionan los principales entregables relacionados al Servicio de Soporte Técnico y Operación de la Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube de IMSS y DRP.

ENTREGABLE	FECHA DE ENTREGA	MEDIO
Transferencia de conocimiento	Como máximo 2 semanas después de la implementación. (Única Ocasión)	Electrónico e impreso
Memorias Técnicas de la configuración e instalación de la plataforma de virtualización.	Como máximo 10 días posteriores al mes en curso.	Electrónico e impreso

Cumplimiento de obligaciones contractuales

Para la documentación de Cumplimiento de Obligaciones contractuales, que permita una fácil y organizada atención de procesos de auditoria por parte de los entes de fiscalización, el **LICITANTE** elaborará en un plazo no mayor a 15 (quince) días hábiles posteriores a la adjudicación del contrato, una matriz de los verbos, pronombres, tiempos y compromisos presentes en el anexo técnico, términos y condiciones, apéndices o documentación complementaria al anexo, así como en la propia oferta del **LICITANTE** ganador, a fin de contar con un listado de todos los verbos de acción, conjunciones, excepciones, interacciones,

consideraciones de tipo y frecuencia de información electrónica que deba incluirse, casos de uso y en su caso especificaciones o excepciones, para convertirlos en los "documentos probatorios de cada obligación establecida en el contrato".

A partir de este listado, de manera conjunta entre el **IMSS** y el **LICITANTE**, en un plazo no mayor a 10 (diez) días hábiles posteriores a la entrega del listado por parte del 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 deductivas aplicables. En estas juntas de gobierno del contrato, el **LICITANTE** deberá exponer al personal **IMSS**, los detalles de la operación, consumos, tendencias, áreas de oportunidad y mejores prácticas susceptibles de incorporarse a la operación y administración del contrato, las cuales serán evaluadas por el **IMSS** y en su caso, autorizadas con o sin modificaciones, para su implementación y operación gradual o inmediata.

Para la exposición y análisis de la información presentada por el **LICITANTE**, éste deberá habilitar al menos 3 pantallas de al menos 75 pulgadas, con todo lo necesario para la presentación de información de la operación de los servicios tecnológicos que permitan exponer de manera gráfica y ágil lo descrito en los dos párrafos anteriores, lo que permitirá contar con información en línea constante de la operación de los servicios contratados incluyendo elementos de análisis y detalles de la operación (parámetros de utilización) de la infraestructura ofertada además de la prestación de los servicios, preferentemente reflejando la operación en términos de infraestructura física o virtual (según corresponda) además de indicadores de negocio que puedan ser descritos desde el alcance de cada contrato.

A. CLÁUSULAS Y CUMPLIMIENTOS

a. Contrato de confidencialidad

El **LICITANTE** en conjunto con el **IMSS** deberá firmar un Contrato de confidencialidad mediante el cual el **LICITANTE** se obliga a no revelar, transferir, compartir ni ceder ningún dato o información de carácter sensible y confidencial que se hayan compartido entre el **LICITANTE** y el **IMSS**.

b. Cláusula de Opción para Obtención de Bienes al cierre de contrato (entregable de infraestructura)

Una vez concluida la prestación del servicio, el **LICITANTE** realizará un proceso de entrega de todo el equipamiento que haya sido incorporado como parte del proyecto. Llámese cualquier componente de hardware/software que integre dicho servicio descrito en el presente documento, así como en la propuesta del proveedor. El **LICITANTE** deberá sujetarse al procedimiento que el **IMSS** requiera para formalizar este proceso.

c. Documentación de cumplimiento de obligaciones

El **LICITANTE** con el objeto de fortalecer la supervisión y vigilancia de la administración del contrato materia del presente servicio y contribuir a las acciones para verificar la procedencia de los pagos, proporcionará un

ANEXOS
DIVISION DE CONTRATOS

soporte especializado para la gestión del conocimiento administrativo relacionado con la prestación de los servicios de Nube **IMSS**.

Para que dicho conocimiento administrativo sea traducido en un activo del **IMSS**, el **LICITANTE** deberá aplicar el modelo de control de contratos definido por la Coordinación de Sistemas de Infraestructura Tecnológica Institucional (o la correspondiente por funciones organizacionales) y ejecutará las acciones que se establecen en dicho modelo como un ejercicio permanente durante la vigencia del contrato. Para tal efecto, se deberá implementar un mecanismo para que dicho soporte especializado encargado de la gestión del conocimiento administrativo de los servicios objeto del presente anexo, cuente oportunamente con cada una de las solicitudes de servicio que se generen en el marco del contrato respectivo, así como respecto de todos los comunicados y documentos existentes entre el **IMSS** y el **LICITANTE** en relación con la prestación de los servicios. Lo anterior, toda vez que los servicios de soporte especializados previstos en ese aparatado están sujetos a flujo de información antes citada.

Lo anterior, con el fin de que el **LICITANTE** elabore los "Reportes de Administración" con corte mensual, que concluya las acciones relacionadas a la facturación presentada durante el periodo de la prestación del servicio, cuyo contenido se señala a continuación:

- **Gestión de los servicios**: Con base en las solicitudes u órdenes de servicio que genere el **IMSS**, el **LICITANTE** incluirá un desglose detallado del trámite que corresponde a la atención de cada una de ellas, en cuanto a su procedencia, tiempos límite de respuestas y demás circunstancias que se encuentren establecidas en el contrato respectivo y que permitan al Administrador del mismo tener control sobre dicha gestión, así como la documentación probatoria del devengo de los servicios, incluyendo toda la documentación o archivos electrónicos que demuestren la prestación del servicio, de conformidad a la funcionalidad solicitada y acorde a los niveles de servicio establecidos, siendo posible entre otros: reportes de monitoreo, disponibilidad, capacidad, desempeño y atención de incidentes, tickets de la mesa, actualizaciones, bitácoras, logs de aplicaciones, entre otros. En caso de que el licitante no cuenta con la documentación probatoria de los servicios devengados, estos no podrán ser facturados.

- **Plataforma de obligaciones:** En este apartado, el **LICITANTE** elaborará un listado que identifique la totalidad de las obligaciones que se encuentran plasmadas en el contrato y sus respectivos anexos relacionados con los servicios. Asimismo, llevará a cabo su clasificación en atención a su importancia y consecuencia en:

  a. Obligaciones principales. Condicionantes del pago y los que están asociados a deductivas
  b. Obligaciones secundarias. No coincidan 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** 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 mismas. 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 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** 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** 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 deductivas, entre otros elementos.
- **Esquema de integración de pagos:** El **LICITANTE** incluirá en los reportes la identificación de los elementos justificativos y comprobatorios que soporten la prestación de servicios durante el periodo que se reporte, conforme a las disposiciones normativas vigentes. Con esta información, el **LICITANTE** integrará la carpeta que soporte la solicitud de pago ante el **IMSS** por la entrega o prestación de los servicios devengados en el periodo mensual correspondiente, para su trámite y gestión por parte del Administrador del contrato, en términos de las facultades con que cuenta para la aceptación de los servicios.
- **Proyección del consumo de los servicios**: Con base en las facturas identificadas para pago, el **LICITANTE** elaborará un modelo gráfico y analítico que registre el consumo mensual real de cada uno de los servicios facturados y que permita un análisis comparativo respecto al consumo programado, a efecto de brindar al administrador del contrato información para la toma de decisiones. Los reportes de administración para la gestión del conocimiento administrativo de los servicios deberán formar parte invariablemente de los documentos justificativos que soportan cualquier pago que se realice durante la vigencia del contrato correspondiente.

22 CRONOGRAMA DE ACTIVIDADES

Las actividades para la ejecución están categorizadas en 4 grandes etapas que se mencionan a continuación.

1. Entrega y recepción de documentación posterior a la adjudicación
2. Mesas de trabajo del inicio del contrato
3. Acuerdos de Niveles de Servicio con otros proveedores del Instituto
4. Establecimiento de matrices de escalación, procedimientos de atención en la mesa de servicio, establecimiento de grupos de soporte.
5. Establecimientos de órdenes de trabajo iniciales
6. Calendario, plan de trabajo, establecimiento de compromisos tales como: instalación, configuración y puesta a punto de la plataforma de virtualización
7. Plan de trabajo para las labores de BCP y DRP
8. Pruebas de BCP y DRP sobre la plataforma de virtualización
9. Mesas de trabajo para el cierre del contrato

23 NIVELES DE SERVICIO

El proceso de Administración del Nivel del Servicio deberá involucrar tanto al **LICITANTE** como al **IMSS** para mantener y monitorear el adecuado funcionamiento del servicio. El **LICITANTE** deberá mantener una revisión continúa de los logros de servicio para garantizar que la calidad del servicio sea mantenida y mejorada permanentemente.

Nivel general de servicio

Los niveles de servicio establecidos que deberá cumplir el licitante en la prestación de los servicios es el siguiente:

El nivel de servicio base para este contrato es de:

Nivel de Disponibilidad	Minutos Indisponibles permitidos en el mes para los servicios del presente contrato
99.982% sobre la plataforma instalada (TIER III)	7.8 minutos

Esta disponibilidad establecida incluye el servicio de soporte técnico en caso de falla en un esquema de 5x8 en días y horarios hábiles con soporte presencial certificado, por lo que en su caso, será exigible la participación de especialistas únicamente en estos horarios, sin embargo, puede requerirse presencia en un esquema 7x24 del personal asociado al servicio, a petición del Instituto.
Los niveles de servicio para la atención tickets, incidentes, atención de requerimientos se detalla a continuación

Criticidad	Tipo de Cobertura	Cobertura	Tiempo de registro del evento (minutos naturales)	Tiempo de diagnóstico (horas naturales)	Tiempo de solución o sustitución a partir del diagnóstico (horas naturales)
Tipo de Criticidad del servicio		Horarios de atención para los incidentes	Tiempo de registro del evento (llamada telefónica / correo electrónico)	Tiempo de diagnóstico del incidente a partir de levantamiento del reporte (considera colocar equipo de respaldo temporal)	Tiempo en el que debe de solucionar o sustituir un equipo, configuración o infraestructura lógica por diagnóstico de falla irreparable o fuera de soporte
Alta	**7x24xVigencia del contrato**	0:00 a 24:00	10	2	2
Media	**5x8 xVigencia del Contrato**	0:00 a 24:00	10	3	4
Baja	**5x8 xVigencia del Contrato**	0:00 a 24:00	10	4	8

El **LICITANTE** cumplirá con los tiempos de respuesta solicitados por el **IMSS**.

Por "TIEMPOR DE REGISTRO DEL EVENTO" se entenderá como el tiempo máximo transcurrido desde el momento en que el **IMSS** o las herramientas de monitoreo automatizadas reportan una falla o desviación en el desempeño de los ambientes virtualizados lógicos (el que ocurra primero), se registre el evento en su herramienta de mesa de servicio y notifique al IMSS el número de ticket para su atención, de acuerdo al procedimiento para el reporte de fallas o de herramientas automatizadas para el monitoreo.

Por "TIEMPO DE DIAGNOSTICO" se entenderá el tiempo máximo transcurrido desde el momento en que el LICITANTE notifique al IMSS el número de ticket para su atención y hasta el momento en que personal del **LICITANTE** efectúe el diagnóstico o determinación del plan de solución y lo haga de conocimiento del **IMSS**.

Por "TIEMPO DE SOLUCIÓN' se entenderá el tiempo máximo transcurrido desde el momento en que el **LICITANTE** efectúe el diagnóstico o determinación del plan de solución, y hasta el momento en que personal del **LICITANTE** ya sea de manera remota o en SITIO, haya finalizado las acciones necesarias para dejar el SERVICIO operando de acuerdo a su funcionalidad normal. En caso de ser necesario, el **LICITANTE** podrá sustituir alguna infraestructura física o virtual de manera total o parcial por otro de igual o superiores características, y podrá realizar las adecuaciones necesarias a la configuración para conseguir su funcionalidad normal de operación.

El **LICITANTE** debe de contar con una base de conocimientos, la cual se deberá actualizar de forma dinámica con el propósito de reducir tiempos de respuesta en los incidentes.

Deductivas por incumplimiento de niveles de servicios

La siguiente tabla clasifica las deductivas aplicables de manera particular a los servicios del presente documento.

Acciones	Nivel de Servicio	Deductiva
Validación de Componentes de Infraestructura física (**)	- A más tardar 24 horas naturales posteriores a la notificación.	- El equivalente a 10% del costo del servicio por deficiencias en la validación de componentes de infraestructura física.
Instalación de Infraestructura Virtual (**)	- A más tardar 24 horas naturales posteriores a la solicitud del servicio, de conformidad al marco (stack) tecnológico definido.	- El equivalente a 10% del costo del servicio por desviaciones de la infraestructura entregada Vs el marco (stack) tecnológico definido.
Configuración y Puesta a Punto de Infraestructura Virtual (**)	- A más tardar 24 horas naturales posteriores a la solicitud de configuración y puesta a punto.	- El equivalente a 10% del costo del servicio por desviaciones de la configuración y puesta a punto de la infraestructura virtual.
Tunning de Infraestructura Virtual (**)	- A más tardar 24 horas naturales posteriores a la solicitud de tunning de infraestructura virtual o en su caso el periodo que se defina de común acuerdo entre el **LICITANTE** y autorizado por el Instituto.	- El equivalente a 10% del costo del servicio por desviaciones de tunning de infraestructura virtual.

Acciones	Nivel de Servicio	Deductiva
Actualización y Mantenimiento de Infraestructura Virtual (**)	- A más tardar 24 horas naturales posteriores a la detección de desviaciones en el desempeño operativo de la infraestructura virtual o en su caso el periodo que se defina de común acuerdo entre el Licitante y autorizado por el Instituto.	- El equivalente a 10% del costo del servicio por desviaciones de actualización o mantenimiento de infraestructura virtual, cuya afectación o impacto sea menor. - El equivalente a 30% del costo del servicio por desviaciones de actualización o mantenimiento de infraestructura virtual, cuya afectación o impacto sea Medio. - El equivalente a 50% del costo del servicio por desviaciones de actualización o mantenimiento de infraestructura virtual, cuya afectación o impacto sea Mayor. Lo anterior, de acuerdo a la matriz de impacto establecida en las mesas de planeación.
Gestión de Incidentes de la Infraestructura Virtual (Lógica)	- De acuerdo a la severidad de afectación y a las matrices de escalación y de impacto definida en las mesas de planeación del arranque. - Nivel de servicio 99.9 de disponibilidad en horario hábil (5x8).	- El equivalente a 2.5% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio. - El equivalente a 10% del costo del servicio por desviaciones en la gestión de incidentes de la infraestructura virtual, cuya afectación o impacto sea menor. - El equivalente a 30% del costo del servicio por desviaciones en la gestión de incidentes de la infraestructura virtual, cuya afectación o impacto sea Medio. - El equivalente a 50% del costo del servicio por desviaciones en la gestión de incidentes de la infraestructura virtual, cuya afectación o impacto sea Mayor. Lo anterior, de acuerdo a la matriz de impacto establecida en las mesas de planeación.

Acciones	Nivel de Servicio	Deductiva
Configuración de Redes y Telecomunicaciones Virtuales	- De acuerdo a la complejidad o en su caso a los tiempos establecidos por el Instituto y el proveedor acorde al impacto definido en las mesas de planeación del arranque.	- El equivalente a 10% del costo del servicio por desviaciones en la Configuración de Redes y Telecomunicaciones Virtuales, cuya afectación o impacto sea menor. - El equivalente a 30% del costo del servicio por desviaciones en la Configuración de Redes y Telecomunicaciones Virtuales, cuya afectación o impacto sea Medio. - El equivalente a 50% del costo del servicio por desviaciones en la Configuración de Redes y Telecomunicaciones Virtuales, cuya afectación o impacto sea Mayor. Lo anterior, de acuerdo a la matriz de impacto establecida en las mesas de planeación.
Aprovisionamiento de Infraestructura Virtual	- A más tardar 24 horas naturales posteriores a la solicitud del servicio, de conformidad al marco (stack) tecnológico definido.	- El equivalente a 10% del costo del servicio por desviaciones de la infraestructura entregada Vs el marco (stack) tecnológico definido.

Acciones	Nivel de Servicio	Deductiva
Servicio de Respaldo y Restauración	- Configuración de políticas, a más tardar 06 horas naturales posteriores a la solicitud del servicio. - Ejecución de respaldos, iniciar a más tardar 3 horas naturales posteriores a la hora indicada en el respaldo para su ejecución, en la política de respaldo asociada. - Ejercicio de restauración, iniciar a más tardar 12 horas posteriores a la solicitud del ejercicio por parte del Instituto. - Restauraciones bajo demanda, iniciar a más tardar 01 hora posterior a la solicitud del Instituto. - La operación del servicio deberá ser 24x7x365, con un nivel de servicio al menos de 99.9%	- El equivalente a 10% del costo del servicio por desviaciones en la restauración de la información Vs el requerimiento realizado por el Instituto (Política de respaldo), cuyo afectación o impacto sea bajo. - El equivalente a 30% del costo del servicio por desviaciones en la restauración de la información Vs el requerimiento realizado por el Instituto (Política de respaldo), cuyo afectación o impacto sea medio. - El equivalente a 50% del costo del servicio por desviaciones en la restauración de la información Vs el requerimiento realizado por el Instituto (Política de respaldo), cuya afectación o impacto sea mayor. Lo anterior, de acuerdo a la matriz de impacto establecida en las mesas de planeación.
Estación de Trabajo Equipada	- A más tardar 02 horas posteriores a la solicitud del servicio.	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido.
Monitoreo y Reporteo de Infraestructura Virtual	- A más tardar 05 días naturales posteriores a la solicitud del servicio. - El detalle y la periodicidad de los reportes serán definidos en las mesas de trabajo al inicio del contrato. - La operación del servicio deberá ser 24x7x365, con un nivel de servicio al menos de 99.9%	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido. Siempre y cuando no haya habido un requerimiento de ventana de mantenimiento debidamente autorizado por el Instituto.

Acciones	Nivel de Servicio	Deductiva
Habilitación y operación de centros de monitoreo en instalaciones del IMSS en Reforma 476 o en las instalaciones que determine el Instituto.	- A más tardar 30 días naturales posteriores a la solicitud del servicio. - La operación del servicio deberá ser 24x7x365, con un nivel de servicio al menos de 99.9%	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido. Siempre y cuando no haya habido un requerimiento de ventana de mantenimiento debidamente autorizado por el Instituto.
Tablero de Consumo Tendencias de Infraestructura Virtual y Gasto	- Para su inicio: A más tardar 20 días naturales posteriores a la solicitud del servicio. - Para su actualización: A más tardar 10 días naturales posteriores a la solicitud del servicio. - La operación del servicio deberá ser 24x7x365, con un nivel de servicio al menos de 99.9%	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido. Siempre y cuando no haya habido un requerimiento de ventana de mantenimiento debidamente autorizado por el Instituto.
Sizing y Arquitectura de Infraestructura Virtual	- La operación del servicio deberá ser 5x8, con un nivel de servicio al menos de 99.9% - Deberá informar que los parámetros de operación exceden los rangos establecidos en las mesas de trabajo al inicio del contrato. - Deberá ejecutar el cambio de arquitectura o redimensionamiento (resizing) previa autorización del Instituto.	- El equivalente a 10% del costo del servicio mensual cuando no informe que los parámetros de operación exceden los rangos establecidos en las mesas de trabajo al inicio del contrato. - El equivalente a 30% del costo del servicio mensual cuando no se ejecute el cambio de arquitectura o redimensionamiento (resizing) previa autorización del Instituto. - El equivalente a 20% del costo del servicio mensual cuando se ejecute el redimensionamiento o el cambio de arquitectura y se presenten afectaciones de baja criticidad. - El equivalente a 30% del costo del servicio mensual cuando se ejecute el redimensionamiento o el cambio de

Acciones	Nivel de Servicio	Deductiva
		arquitectura y se presenten afectaciones de mediana criticidad. - El equivalente a 50% del costo del servicio mensual cuando se ejecute el redimensionamiento o el cambio de arquitectura y se presenten afectaciones de alta criticidad. El nivel de afectación se determinará de conformidad a las matrices de impacto que se definan en las mesas de trabajo al inicio del contrato.
Administrador de Proyectos	- Reporte diario de avance de proyectos (el detalle se definirá en las mesas de planeación del arranque). - Reunión semanal de seguimiento de proyectos que incluya además de lo anterior presupuesto, recursos y tiempo.	- El equivalente a 10% del costo mensual del servicio por deficiencias en la veracidad del reporte y la información.
Representante de Servicios en Sitio	- Informe diario de avance de proyectos que incluya presupuesto, recursos, tiempo, incidentes, cambios, problemas y desviaciones (el detalle se definirá en las mesas de planeación del arranque). - Reunión semanal de seguimiento de proyectos.	- El equivalente a 10% del costo mensual del servicio por deficiencias en la veracidad del informe.

Acciones	Nivel de Servicio	Deductiva
Documentación de Cumplimiento de Obligaciones	- La documentación del cumplimiento de obligaciones, el detalle se definirá en las mesas de planeación del arranque. - Elaboración y firma de los Acuerdos Operacionales (OLAs) durante las mesas de planeación (a más tardar a 03 semanas posteriores a la notificación del fallo). - Elaboración de reporte de cumplimiento de los acuerdos operacionales (por proveedor). - Elaboración mensual del cumplimiento de obligaciones.	- Por deficiencias en la veracidad de cada documento que acredite el cumplimiento de obligaciones (entregables), se aplicará una deductiva equivalente a 5% del costo mensual del servicio de infraestructura virtual.
Repositorio Documental	- El inicio de operaciones del Repositorio Documental será en la fecha establecida en las mesas de planeación del arranque. -La actualización periódica del Repositorio Documental deberá realizarse de acuerdo a lo establecido en las reuniones de gobierno del contrato, las cuales se efectuarán semanalmente. - La operación del repositorio documental deberá ser 5x8, con un nivel de servicio al menos de 99.9%	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido. - Por deficiencias en la veracidad de la documentación contenida en el repositorio, se aplicará una deductiva equivalente a 10% del costo mensual del servicio.

Acciones	Nivel de Servicio	Deductiva
Servicio de Entrega al Cierre de Contrato	- La documentación del cumplimiento de obligaciones, el detalle se definirá en las mesas de planeación del arranque. -Listado de compromisos contractuales y el estado que guardan al cierre del contrato, cumplimiento de entregables.	- Por deficiencias en la veracidad de cada documento que acredite el cumplimiento de obligaciones (entregables), se aplicará una deductiva equivalente a 5% del costo mensual del servicio de infraestructura virtual.
Transferencia de Conocimiento y Adiestramiento Tecnológico	- Las fechas de entrenamiento se definirán en las mesas de planeación del arranque.	- Por deficiencias en la impartición del entrenamiento tecnológico se aplicará una deductiva del 30% del costo del servicio, la deficiencia se determinará mediante la aplicación de encuestas de satisfacción a los participantes del curso, en caso que el promedio de la evaluación sea menor a 80%.
Contrato de Confidencialidad	- Cumplimiento de la confidencialidad por parte de ambas instituciones durante la vigencia establecida en el convenio de confidencialidad.	- En caso del incumplimiento de la confidencialidad establecida, se aplicará una deductiva equivalente al 10% del valor máximo del contrato.
Soporte empresarial de la solución de virtualización que incluya transferencia de conocimiento.	- La contratación del soporte empresarial deberá ser a más tardar en la fecha establecida en las mesas de trabajo de inicio del contrato. - La operación del soporte deberá ser el establecido entre el IMSS y el LICITANTE Adjudicado en las mesas de trabajo de inicio del contrato. - Las fechas de entrenamiento se definirán en las mesas de planeación del	- El equivalente a 10% del costo mensual del servicio de soporte fuera del nivel de servicio establecido entre el IMSS y el LICITANTE Adjudicado en las mesas de trabajo de inicio del contrato. - Por deficiencias en la impartición del entrenamiento tecnológico se aplicará una deductiva del 30% del costo del servicio, la deficiencia se determinará mediante la aplicación de encuestas de satisfacción a los participantes del curso, en caso que el promedio de la evaluación sea menor a 80%.

Acciones	Nivel de Servicio	Deductiva
	arranque.	
CMDB de Infraestructura Lógica	- La entrega de la CMDB inicial se deberá realizar en el plazo acordado en las mesas de trabajo al inicio del contrato. - La actualización periódica de los elementos de configuración (CMDB) deberá realizarse de acuerdo a lo establecido en las reuniones de gobierno del contrato, las cuales se efectuarán semanalmente.	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido.

Acciones	Nivel de Servicio	Deductiva
Base de FAQs para Publicación de Soluciones Rápidas	- La entrega de la Base de FAQs para Publicación de Soluciones Rápidas inicial se deberá realizar en el plazo acordado en las mesas de trabajo al inicio del contrato. - La actualización periódica de los elementos de la Base de FAQs para Publicación de Soluciones Rápidas deberá realizarse de acuerdo a lo establecido en las reuniones de gobierno del contrato, las cuales se efectuarán semanalmente.	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido.
Repositorio de Imágenes de Contenedores	- La entrega de la Base de FAQs para Publicación de Soluciones Rápidas inicial se deberá realizar en el plazo acordado en las mesas de trabajo al inicio del contrato. - La actualización periódica de los elementos de la Base de FAQs para Publicación de Soluciones Rápidas deberá realizarse de acuerdo a lo establecido en las reuniones de gobierno del contrato, las cuales se efectuarán semanalmente.	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido.

(**) El marco de referencia para estas definiciones, serán perfeccionados o particularizados en las mesas de trabajo realizadas al inicio del respectivo contrato, sin embargo, de manera general, tendrán el siguiente alcance:

Validación de Componentes de Infraestructura física: Se refiere a la actividad de comprobar que la infraestructura física entregada por parte del **LICITANTE** adjudicado correspondiente a la infraestructura física, cumple con las características solicitadas por el **IMSS** y se encuentra listo para ser configurado de manera lógica o virtual.

Instalación de Infraestructura Virtual: Se refiere a la actividad de virtualización de la infraestructura física entregada por parte del **LICITANTE** adjudicado correspondiente a la infraestructura física, de tal manera que, pueda entregar servicios lógicos o virtuales utilizables por el IMSS, en general, son instalaciones por default o con parámetros de fábrica, que si bien permiten un uso por parte del IMSS, podrían ser optimizados en el contexto del ecosistema tecnológico Institucional.

Configuración y Puesta a Punto de Infraestructura Virtual: Se refiere a la actividad(es) de realizadas por parte del LICITANTE para que la infraestructura virtualizada pueda ser usada para los fines definidos por el IMSS, optimizando las instalaciones por default o con parámetros de fábrica, que si bien permiten un uso por parte del IMSS, podrían ser optimizados en el contexto del ecosistema tecnológico Institucional, a fin de garantizar la continuidad operativa de esta infraestructura virtual dentro del ecosistema operativo.

Operación de Infraestructura Virtual: Se refiere a la actividad de mantener la continuidad operativa de la infraestructura virtualizada dentro de los parámetros de operación y desempeño establecidos para este fin.

Tunning de Infraestructura Virtual: Se refiere al ajuste y optimización periódico (al menos cada tres meses o cada que se detecte un incidente de desviación de los niveles de desempeño establecidos en el presente documento, incluyendo el correcto dimensionamiento de la infraestructura física o virtual) de la infraestructura virtualizada (hipervisor, contenedor, sistemas operativos huésped, software especializado, sistemas, aplicativos, servicios, bases de datos, web services, servidores de aplicación, balanceadores, es decir, todo aquello que se encuentre contenido en la infraestructura física entregada para su virtualización) en operación y que permita tener un mejor desempeño de los ambientes virtualizados de conformidad a los parámetros definidos en el ecosistema tecnológico Institucional.

Actualización y Mantenimiento de Infraestructura Virtual: Se refiere a las actividades de mantener la infraestructura virtualizada (actualizaciones, parches, configuraciones, parámetros, dimensionamiento y todo lo relacionado a la correcta operación del sistema o de los servicios virtualizados) en las últimas versiones liberadas y estables por parte del fabricante del hipervisor, contenedor, sistemas operativos huésped, software especializado, sistemas, aplicativos, servicios, bases de datos, web services, servidores de aplicación, balanceadores, es decir, todo aquello que se encuentre contenido en la infraestructura física entregada para su virtualización.

Gestión de Incidentes de la Infraestructura Virtual (Lógica): Se refiere a todas a las actividades relacionadas al seguimiento y solución de los eventos, incidentes y problemas que se presenten en la infraestructura virtualizada o en uno de sus componentes o hipervisor, contenedor, sistemas operativos huésped, software especializado, sistemas, aplicativos, servicios, bases de datos, web services, servidores de aplicación, balanceadores, es decir, todo aquello que se encuentre contenido en la infraestructura física entregada para su virtualización.

Configuración de Redes y Telecomunicaciones Virtuales: Se refiere a la actividad(es) de realizadas por parte del LICITANTE para que la infraestructura virtualizada de Redes y Telecomunicaciones pueda ser usada para los fines definidos por el IMSS, optimizando las instalaciones por default o con parámetros de fábrica, que si bien permiten un uso por parte del IMSS, podrían ser optimizados en el contexto del ecosistema tecnológico Institucional, a fin de garantizar la continuidad operativa de esta infraestructura virtual dentro del ecosistema operativo.

24 REQUERIMIENTOS DE ARQUITECTURA TECNOLÓGICA

N/A

25 RESTRICCIONES E INTERFACES CON OTROS ELEMENTOS

N/A

26 PROCESO DE ENTREGA AL TÉRMINO DEL CONTRATO

Una vez concluida la prestación del servicio, el **LICITANTE,** entre otras cosas, realizará un proceso de entrega de todo el equipamiento, software, configuración, desarrollos, CMDB, base de datos de conocimiento, diagramas, bases de conocimiento de configuración de: hipervisor, contenedor, sistemas operativos huésped, software especializado, sistemas, aplicativos, servicios, bases de datos, web services, servidores de aplicación, balanceadores, monitoreo y en general de todas las herramientas y funcionalidades de todo lo que haya sido incorporado como parte del proyecto o en su caso, producto del servicio, incluyendo cualquier componente de hardware/software que integre dicho servicio descrito en el presente documento, así como en la propuesta del proveedor. El **LICITANTE** deberá sujetarse al procedimiento que el **IMSS** requiera para formalizar este proceso.

27 FORMA DE PAGO DE LOS SERVICIOS

La forma de pago establecida para este servicio, será de un pago mensual por los servicios devengados y entregados al IMSS por parte del LICITANTE,

Mínimos y máximos :

Concepto	Mínimo	Máximo
Red Hat Ansible Automation, Standard (100 Managed Nodes)	1.00	1.00
Red Hat Virtualization Suite with Guests and Management (2-sockets), Standard	12.00	24.00
Red Hat OpenShift Container Platform with Integration, Standard (64 Cores or 128 vCPUs)	2.00	4.00
Red Hat OpenShift Container Storage, Standard (2 Core)	12.00	24.00
Servicio de Instalación de RHVS	12.00	24.00
Servicio de Instalación de RHOP	4.00	8.00
Enlace de 1 GB	2.00	4.00
Servicio de Configuración de Redes Virtuales	1.00	1.00
Punto Neutro	1.00	2.00
Servicio de Soporte a Software	2.00	2.00
Servicio de Asesoría Tecnica Especializada en Sitio	2.00	2.00

La volumetría que se proporciona es exclusivamente para efectos de cotización y no necesariamente refleja los requerimientos del Instituto, por lo que no se deberá considerar como las cantidades a contratar. La cantidad de servicios a contratar se determinará por el presupuesto mínimo y máximo establecido.

28 FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN

Responsables de Elaboración

Héctor Martínez Valenzuela
Titular de la División de Telecomunicaciones
03/12/2019

Alejandro Paniagua Ramírez
Titular de la División de Administración de Riesgos Tecnológicos
03/12/2019

Carlos Francisco Ramírez del Rivero,
Titular de la División de Administración y Continuidad de la Operación
03/12/2019

Héctor Javier Reyes Oropeza
Titular de la División de Administración, Procesamiento y Almacenamiento
03/12/2019

Javier Cortés López
Titular de la Coordinación Técnica
de Operación de Servicios
Tecnológicos
03/12/2019

Carlos Calderón Zacarias
Titular de la Coordinación Técnica
de Redes y Telecomunicaciones
03/12/2019

Responsables de Aprobación

Eduardo Oropeza Ortiz
Titular de la Coordinación de
Sistemas de Infraestructura
Tecnológica Institucional
03/12/2019

ANEXOS
DIVISION DE CONTRATOS

SIN TEXTO

	INSTITUTO MEXICANO DEL SEGURO SOCIAL **DIRECCIÓN DE ADMINISTRACIÓN** **UNIDAD DE ADQUISICIONES E INFRAESTRUCTURA** **COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS** **COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS**	**Contrato Número P0M0017**

ANEXO 2 (DOS)

"PROPUESTA TÉCNICA, PROPUESTA ECONÓMICA Y ACTA DE NOTIFICACIÓN"

ANEXOS
DIVISION DE CONTRATOS

EL PRESENTE ANEXO CONSTA DE **70** HOJAS INCLUYENDO ESTA CARÁTULA

SIN TEXTO

IPICYT

INSTITUTO POTOSINO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA, A.C.

"Servicio de Soporte técnico y operación de la Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube IMSS y DRP"

Perteneciente al Instituto Mexicano del Seguro Social (IMSS)

ANEXOS
DIVISION DE CONTRATOS

CONTENIDO

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

ANEXOS
DIVISION DE CONTRATOS

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

IPICYT
INSTITUTO POTOSINO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA, A.C.

CNS
CENTRO NACIONAL DE SUPERCÓMPUTO
IPICYT

CARTA DE PRESENTACIÓN

San Luis Potosí, S. L. P., a 20 de diciembre del 2019
Asunto: Propuesta Comercial
Clave de Propuesta: CNS 2019-000045

Titular de la División de Investigación de Mercados
de Adquisiciones y Arrendamientos
Instituto Mexicano del Seguro Social (IMSS)

PRESENTE

Agradezco de antemano la oportunidad que nos brinda al colaborar en los proyectos de tecnología de información de su organización. En atención a los requerimientos proporcionados pongo a su disposición, esta propuesta técnica y económica para llevar a cabo el **"Servicio de Soporte Técnico y Operación de la Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube de IMSS y DRP"**

Aprovecho para comentar que el Centro Nacional de Supercómputo cuenta con la infraestructura, personal técnico especializado, procedimientos y equipos suficientes y adecuados para cubrir las necesidades de su organización, a fin de garantizar que se proporcione con calidad, oportunidad y la eficiencia requerida.

Sin otro particular, quedo a sus órdenes para cualquier comentario o aclaración.

Atentamente

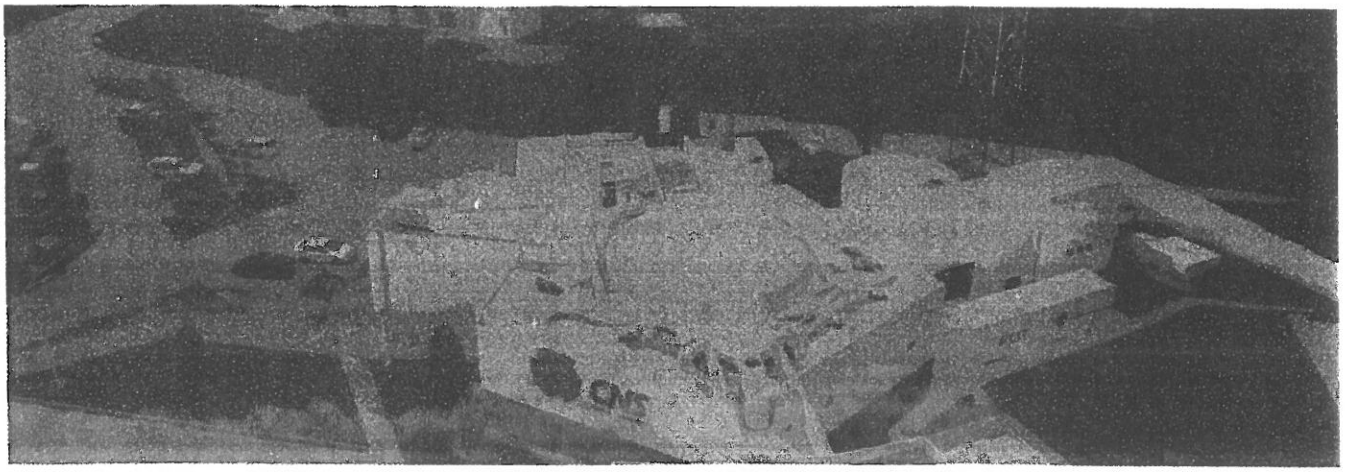
Dr. Luis Antonio Salazar Olivo
Director General y Representante Legal
Del Instituto Potosino de Investigación Científica y Tecnológica, A.C.
CNS-IPCYT
olivo@ipicyt.edu.mx
Tel. (444)8342000 ext. 2101

IPICYT
INSTITUTO POTOSINO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA, A.C.

ACERCA DE NOSOTROS

Somos un Laboratorio Nacional inaugurado en agosto del 2006, que nace para atender la demanda de la comunidad científica en materia de Cómputo de Alto Rendimiento (HPC por sus siglas en inglés). Iniciamos participando en proyectos utilizando nuestra infraestructura, los cuales reditúan en ingresos propios, con el fin de mantener en operación un Centro de Supercómputo de vanguardia tecnológica. Somos reconocidos como líderes a nivel regional con presencia nacional e internacional, dedicados a proveer soluciones tecnológicas integrales y personalizadas en Supercómputo, informática y redes. Apoyados de infraestructura que nos permite contar con la capacidad para desarrollar proyectos de alto impacto en la sociedad para los sectores gubernamental, privado, educativo y científico por medio de personal altamente capacitado y certificado en las mejores prácticas.

Localizados en el corazón de México, la ciudad capital de San Luis Potosí, en el **CNS-IPCYT** poseemos una provechosa ubicación en el territorio mexicano debido a que nos encontramos en un punto intermedio entre las tres ciudades más importantes del país: la Ciudad de México, Monterrey y Guadalajara; y entre cuatro grandes puertos de altura: Tampico, Altamira, Manzanillo y Mazatlán.



Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

REPRESENTANTES Y OFICINAS

Las oficinas desde donde brindamos atención a nuestros clientes se encuentran ubicadas en:

Camino a la Presa San José 2055,

Col. Lomas 4a. secc.

C.P. 78216

San Luis Potosí, S. L. P.

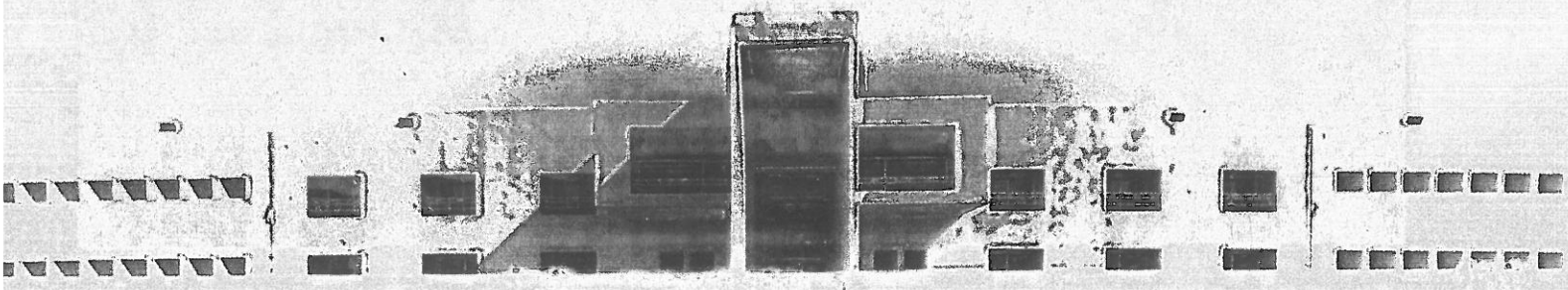
Tel. +52 (444) 834 20 00

Atención al Cliente:

clientes@CNS-IPCYT.mx

http://www.CNS-IPCYT.mx

Desde San Luis Potosí: (444) 834 20 00



PROPUESTA TÉCNICA

1. OBJETIVO

Aprovisionar las herramientas tecnológicas necesarias que permitan al **IMSS** contar con software para la virtualización, almacenamiento de objetos en una nube publica y equipamiento de telecomunicaciones y seguridad de la información.

2. ALCANCE

El **CNS-IPCYT** entregará los componentes tecnológicos solicitados en el presente documento al día natural siguiente del fallo. Para la entrega de la solución propuesta, se contará con los siguientes componentes, los cuales serán instalados, configurados y puesta a punto por el **CNS-IPCYT**:

- Servicios de Operación.
- Unidad de Licenciamiento de Virtualización Red Hat o Similar
- Unidad de Almacenamiento de Objetos sobre plataforma de nube pública.
- Servicio de Respaldo y Recuperación de Información.
- Servicio de Operación de Infraestructura de Seguridad Informática.
- Unidad integral de conmutación de datos y de protección contra amenazas y detección de intrusos.
- Unidad Integral de Balanceo de Cargas en Comunicaciones.
- Unidad Integral de Punto Neutro.
- Unidad de enlace dedicado con una capacidad de 5Gbps.
- Unidad de Soporte
- Transferencia de Conocimiento y Adiestramiento Técnico
- Repositorios.
- Soporte, Operación y Monitoreo de Componentes Lógicos durante la Fase de Pruebas para la Migración.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Soporte, Operación y Monitoreo de Servicios Digitales, así como sus componentes lógicos sobre las plataformas de código abierto.
- Diseño y Pruebas de un Plan de Recuperación de Desastres y un Plan de Continuidad del Negocio para el **IMSS**

3. CARACTERÍSTICAS GENERALES

Como parte de los requerimientos, el **CNS-IPCYT** considerará el suministro, instalación y puesta en operación de la solución propuesta, incluyendo las últimas versiones de software, firmware y licenciamiento correspondiente debidamente habilitado. Todo el equipamiento de hardware y software que se suministre será interoperable y trabajará de forma transparente, con el objeto de garantizar la adecuada integración, interacción y compatibilidad entre componentes.

El **CNS-IPCYT** incluirá todos los cables, accesorios y/o aditamentos de hardware-software necesario para la correcta operación y funcionalidad de la solución propuesta, así como los kits de montaje para gabinete de 19" y 42".

El **CNS-IPCYT** optimizará los recursos y configuraciones de la red, previa instalación del equipamiento de hardware y software que suministre. Asimismo, tomará las debidas precauciones para evitar cortes de servicio en la etapa de instalación de la solución.

3.1. SERVICIOS DE OPERACIÓN

El objetivo de la presente propuesta es establecer las especificaciones, calendarios, niveles de servicio, arquitecturas y lineamientos técnicos para la contratación de los servicios necesarios para la operación de la infraestructura lógica.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.1.1. GESTIÓN Y RESOLUCIÓN DE INCIDENTES, ASÍ COMO ATENCIÓN DE SOLICITUDES RELACIONADAS A LA INFRAESTRUCTURA VIRTUAL.

El **CNS-IPCYT** implementará un punto único de contacto para recibir, registrar, categorizar, dar seguimiento y generar información de los procesos de Gestión de Requerimientos, Gestión y resolución de Incidentes, Gestión de Cambios y Gestión de Problemas, relacionados a los servicios de infraestructura virtual y apegado a los procesos ITIL para la atención de problemas, incidentes y solicitudes con una cobertura de 7x24x365. A continuación, se describen de manera enunciativa más no limitativa, algunos de los eventos que reportarán en la Mesa de Servicio:

- Falla en componentes virtuales
- Degradación del desempeño en las aplicaciones, componentes o servicios virtuales
- Fallas y/o degradación de funcionamiento en Sistema Operativo, Bases de Datos, comunicaciones o cualquier componente virtual
- Cualquier falla o degradación que se detecte en los servicios o la infraestructura lógica relacionados con el servicio de migración o DRP

A fin de que el registro de un ticket, categorización y asignación se realice en el menor tiempo posible y se proporcione la información necesaria suficiente para su atención, el **CNS-IPCYT** realizará las acciones, en conjunto con el **IMSS**, para que cuente con la siguiente información que configurará en la solución tecnológica:

- Guion de atención y catálogo de servicios.
- Matriz de escalamiento.
- Guiones de atención al primer nivel de soporte y/o recabar la información requerida por los grupos de soporte para la atención del ticket.
- Categorizaciones de casos
- Grupos de soporte

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

La Mesa de Servicio estará disponible con los agentes necesarios para recibir y gestionar los casos en un horario de servicio 7x24x365. El **CNS-IPCYT** será responsable de contar con la cantidad de agentes capacitados suficientes para atender la demanda en los diferentes turnos.

El **CNS-IPCYT** proporcionará los mecanismos necesarios para realizar la integración necesaria con de la mesa de servicios ofertada hacia la mesa de servicios Institucional.

Las herramientas, soporte técnico, personal, infraestructura y proceso de atención de la Mesa de Servicio ofertada al **IMSS** estarán personalizados para la atención al **IMSS**, garantizando la continuidad, seguridad y confidencialidad.

El proceso de atención de la Mesa de Servicio será propuesto por el **CNS-IPCYT** y en su caso, adecuado y o autorizado por el **IMSS**.

Los tickets generados por la Mesa de Servicio serán despachados hacia grupos de soporte establecidos por categorización acorde a lo definido entre el Instituto y el **CNS-IPCYT**, cuidando en todo momento lo siguiente:

- El **CNS-IPCYT** contará con una herramienta automatizada para la detección de incidentes o eventos, su registro, notificación, administración, seguimiento y todo lo necesario hasta su resolución, incluyendo mecanismos electrónicos para el seguimiento del avance en la resolución del incidente.
- La Mesa de Servicio despachará inmediatamente el ticket con los grupos de soporte definidos para la atención del evento reportado.
- Todos los tickets se registrarán el horario en que sean creados para el seguimiento de atención y servicio.
- Los tickets serán cerrados hasta que el incidente o el evento que lo generó haya sido solucionado por completo y confirmado por parte del Instituto, por cualquiera de

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

los canales que habilite la mesa, siempre y cuando se genere evidencia de la confirmación del usuario.

Los tiempos de atención y solución proporcionados por el **CNS-IPCYT**, tanto para solicitudes como para incidentes o problemas serán validados y autorizados por el **IMSS** en las mesas de trabajo al inicio del contrato.

3.1.2. PRODUCTOS

Durante los 10 días naturales al mes vencido, el **CNS-IPCYT** enviará al **IMSS** el reporte impreso y firmado por el apoderado legal del **CNS-IPCYT**, referente a los tickets generados en el mes vencido. Dicho reporte tendrá al menos los siguientes campos:

- Numero de ticket.
- Fecha y hora de creación.
- Descripción de lo reportado.
- Nombre o nombres del personal que atendieron el ticket.
- Descripción de la solución y en su caso, reporte postmortem.
- Fecha y hora de la solución.
- Fecha y hora el cierre.
- Tiempo de atención del incidente, requerimiento o ticket.
- Nivel de servicio definido para este tipo de incidente.
- Tiempos acumulados de afectación para este tipo de incidente en el mes en curso.
- En su caso, posible deductiva o pena convencional correspondiente.

3.1.3. ENTREGA Y OPERACIÓN DE SERVICIOS

El **IMSS** requiere contar con el servicio de mantenimiento preventivo y/o correctivo para todas las plataformas tecnológicas virtuales que forman parte del Servicio.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

El **CNS-IPCYT** contará con un Centro de Atención permanente durante las 24 horas del día y durante la vigencia del contrato, proporcionando el soporte técnico que corresponda al horario y vigencia de la contratación del servicio, a través del cual el **IMSS** podrá levantar reportes para solicitar soporte y asesoría técnica telefónica (ilimitada e inmediata).

El **CNS-IPCYT** brindará un tiempo de respuesta inmediato catalogando por grado de severidad de la contingencia presentada, comprometiéndose a un tiempo máximo de resolución indicando en los niveles de servicio; asimismo el **IMSS** podrá solicitar al **CNS-IPCYT** que el servicio se realice en el horario más conveniente para la Organización.

En caso de que el **CNS-IPCYT** no pueda resolver el problema y se requiera el apoyo directo del fabricante, el **IMSS** tendrá acceso por medio del **CNS-IPCYT** a los servicios de soporte y atención del fabricante, así como acceso a su centro de atención.

El **CNS-IPCYT** considerará en sus propuestas técnica y económica, la asignación de los recursos técnicos, humanos y de infraestructura necesarios para resolver, a partir del inicio del contrato toda solicitud referente a este punto y deberá prestarse a todas las plataformas tecnológicas virtuales que forman parte del servicio.

Los Mantenimientos preventivos y/o correctivos a la infraestructura virtual serán supervisados por los recursos provistos por el **CNS-IPCYT**.

El servicio de mantenimiento preventivo y/o correctivo consistirá de manera enunciativa, más no limitativa, de las siguientes actividades:

- Reparación, reinstalación y/o reemplazo de la infraestructura virtual.
- Instalación y/o reinstalación de software institucional y de parches, fixes, actualización, incorporación al directorio activo, entre otros.
- Restauración de configuraciones y parámetros.
- Elaboración de análisis, estudios, diagnósticos y pruebas para la detección de causales que tengan como consecuencia un mal funcionamiento de los equipos

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

físicos y lógicos considerados en este contrato, siendo obligación del **CNS-IPCYT** la entrega de alternativas de solución.

Los mantenimientos preventivos y/o correctivos se realizarán cuantas veces sea necesario en función a las eventualidades o fallas que se presenten durante la vigencia del contrato.

3.1.4. SERVICIOS DE MANTENIMIENTO PREVENTIVOS Y/O CORRECTIVOS

El **CNS-IPCYT** considerará los mantenimientos preventivos y/o correctivos necesarios en caso de falla de alguna de los elementos de infraestructura lógica en los tiempos de atención y niveles de servicio solicitados.

El **CNS-IPCYT** reconfigurará, instalará o en su defecto reemplazará los componentes de infraestructura lógica dañados y restablecer los servicios operativos de acuerdo a la criticidad, el cual se detalla la sección de "Administración del Nivel de Servicio".

La infraestructura lógica que el **CNS-IPCYT** reconfigure o instale será de las mismas características que el activo degradado o dañado.

En el caso de los mantenimientos preventivos y/o correctivos cumplirán con lo siguiente:

- Durante las actividades de mantenimiento preventivo y/o correctivo, el **CNS-IPCYT** llevará a cabo rutinas de diagnóstico del buen funcionamiento de la infraestructura lógica, a fin de garantizar el correcto funcionamiento de todos los equipos. En caso de identificar alguna anomalía con alguno de los equipos, emitirá recomendaciones al **IMSS** para corregir la falla, previo visto bueno del **IMSS**.
- El **CNS-IPCYT** llevará a cabo el diagnóstico para garantizar el correcto funcionamiento de todas las tarjetas, interfaces, cables y demás aditamentos que conforman la base de infraestructura lógica, asimismo en caso de existir deberá localizar y corregir las fallas.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Dentro del programa de operación, realizará las actividades inherentes a los respaldos de configuración de todos los equipos. Dichos respaldos serán entregados para su resguardo al personal que designe el **IMSS**.
- El **CNS-IPCYT** definirá en conjunto con el **IMSS** las ventanas de mantenimiento para la realización de las actividades de mantenimiento correctivo, mediante un plan de trabajo y documentarlo a través de un control de cambios (RFC "Request for Change").

El **CNS-IPCYT** optimizará los recursos y configuraciones de la red y de seguridad, previa instalación de las configuraciones de infraestructura lógica que suministre. Asimismo, tomará las debidas precauciones para evitar interrupciones en el servicio en la etapa de planeación y pruebas de la migración e instalación de la infraestructura lógica y DRP.

3.1.5. PROCEDIMIENTO PARA REPORTE DE FALLAS

El **CNS-IPCYT** contará con una herramienta electrónica para la detección automatizada de incidentes o eventos en la infraestructura virtual, generando de manera automática registro en la herramienta de mesa de servicio, así como los alertamientos al personal del **IMSS** establecidos en las mesas de trabajo al inicio del contrato.

El reporte de fallas será en cualquier horario (7X24X365 durante la vigencia del contrato). El tiempo estipulado para restituir el servicio dependerá del tipo de falla que se presente, el tiempo de resolución de falla se indica en el apartado de Niveles de Servicio.

El **CNS-IPCYT** considerará para la implementación de la infraestructura lógica, incluyendo como mínimo las siguientes actividades:

- Plan de implementación de la infraestructura lógica.
- Instalación de los equipos.
- Interconexión de la infraestructura lógica.
- Configuración tipo de la infraestructura.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Configuración de protocolos.
- Configuración de ruteo.
- Configuración de reglas.
- Configuración de QoS.
- Configuración de multicast en la red para transmitir señales de voz, datos y video.
- Migración de configuraciones de la infraestructura lógica anterior a la infraestructura lógica nueva.
- Configuración de parámetros básicos para monitoreo y administración.
- Configuración para protección de ataques conocidos.
- Configuración de alta disponibilidad.
- Configuración de temas de seguridad lógica.
- Configuración y puesta a punto de los activos tecnológicos lógicos.
- Aplicación de las mejores prácticas de la industria en las materias de infraestructuras tecnológicas virtuales en comento.
- Migración de infraestructura lógica.

Y todas aquellas tareas o configuraciones necesarias en la implementación que el **IMSS** considere necesarias para su correcta operación.

3.1.6. ADMINISTRACIÓN DE SOPORTE REMOTO

Con la finalidad de proporcionar soporte técnico a las diversas infraestructuras tecnológicas del **IMSS**, el **CNS-IPCYT** considerará hacer uso de herramientas de soporte remoto, la cual, permita gestionar apoyo de otros ingenieros a distancia para que los incidentes presentados puedan ser resueltos de manera inmediata en sitio o donde sea necesaria la intervención de especialistas de soporte de nivel superior.

En caso de que el apoyo remoto sea necesario, este será aprobado de manera previa por el **IMSS** mediante los mecanismos electrónicos que proponga el **CNS-IPCYT** y sean autorizados por el Instituto en las mesas de trabajo al inicio del contrato.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.1.7. POLÍTICAS Y PROCEDIMIENTOS

En coordinación el **CNS-IPCYT** y el **IMSS**, definirán los procesos y procedimientos relacionados a la atención de llamadas, escalamiento y todos aquellos procesos que definan la operatividad interna del servicio, alineándose a la normatividad que le aplique (MAAGTICSI o la normatividad aplicable vigente). Una vez definidos será responsabilidad del **CNS-IPCYT** el implementarlos y ejecutarlos durante toda la duración del contrato.

3.2. SERVICIO DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN

El **CNS-IPCYT** habilitará, implementará, configurará, administrará, operará, monitoreará y dará soporte a la plataforma de respaldos siendo de manera enunciativa más no limitativa, incluyendo los siguientes conceptos:

- Niveles de protección tipo RAID 5 o superior y contar con discos hotspare, que evite pérdida de datos.
- Garantizar el aprovechamiento de las redes de conectividad LAN y SAN para las funciones de respaldos.
- Contar con conectividad FC y Ethernet, con soporte da los diversos medios de almacenamiento ofertados, con funciones de deduplicación (compresión) de los datos a respaldar.
- Garantizar la disponibilidad y su mantenimiento no disruptivo dando continuidad al servicio de respaldo y restauración de la información.
- Utilizar algoritmos de deduplicación de datos para almacenar la información, que cumplan las siguientes características:
    - La deduplicación de los datos respaldados debe ser "en línea", sin que represente este proceso una tarea posterior de la ejecución del mismo.
    - El mencionado proceso de deduplicación no deberá representar un espacio adicional temporal.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- El proceso de deduplicación deberá distribuirse en el origen y en el destino a través de los protocolos Ethernet y FC en una red local independiente con un componente de comunicaciones dedicado, de manera que este proceso no afecte la operación de la plataforma virtualizada.

- Soportar el escenario de recuperar la información en un sitio alterno en caso de que el sitio principal presente algún problema que impida la operación.
- El **CNS-IPCYT** establecerá de manera conjunta con el Instituto, un esquema de respaldos y restauración de la información, en los servicios de las bases de datos y de carpetas (datos no estructurados) contenida en la plataforma de virtualización.
- El respaldo será en línea ("En caliente") del total de las bases de datos.
- El respaldo se realizará con periodicidad diaria, semanal y mensual de conformidad a lo definido en la solicitud de respaldo y restauración definida por el Instituto.
- Los respaldos diarios tendrán una retención de 7 días, los semanales de 4 semanas, los mensuales de 3 meses y el anual de 1 año o en su caso, los que se determinen por las áreas de negocio del Instituto.
- Los respaldos se realizarán en medios externos a la plataforma de virtualización, siendo posible la utilización de medios magnéticos o similares como almacenes mecánicos (discos duros) integrados en plataformas de almacenamiento.
- El **CNS-IPCYT** contará con una cintoteca, al interior de su Centro de Datos, así como una cintoteca externa de respaldo, para lo cual el Instituto definirá las políticas de respaldo a seguir.
- La restauración será de forma completa e incluso por elemento, por ejemplo, se podrá recuperar un solo archivo de una carpeta o se podrá recuperar una sola tabla de una base de datos (excepto para los contenedores).
- La restauración no se encimará o sobrescribirá la información que en esos momentos esté en línea, por consiguiente, permitirá al personal del **IMSS** copiar de forma personalizada la información recuperada.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Permitir la replicación de datos entre dos o más equipos a través de la WAN y la replicación debe satisfacer los siguientes puntos:

  a) Replicar datos deduplicados: es decir la replicación debe ocurrir después de los procesos de deduplicación con el objeto de reducir la cantidad de datos a enviar por el enlace WAN y por ende demandar un menor ancho de banda para el proceso.

  b) La replicación se efectuará de forma bidireccional, es decir de un equipo local a otro equipo remoto y viceversa

El **CNS-IPCYT** entregará de forma diaria, un reporte de la ejecución de los respaldos en el cual identifique los exitosos de los fallidos. En caso de falla recurrente (3 ocasiones consecutivas) del mismo proceso de respaldo sin análisis ni ejecución de medidas correctivas, será causa de la aplicación de deductivas.

La solución que brinda el **CNS-IPCYT** incluirá todos los componentes físicos y lógicos necesarios para su operación a fin de cumplir con los niveles de servicio establecidos.

En caso de falla de algún componente del equipo utilizado, el contenido almacenado debe poder regenerarse utilizando niveles de protección adecuada para el servicio.

3.3. SERVICIO DE OPERACIÓN EN INFRAESTRUCTURA DE SEGURIDAD INFORMÁTICA

3.3.1. SEGURIDAD LÓGICA

3.3.1.1. DISEÑO DE LA ARQUITECTURA DE LA SEGURIDAD.

Con la finalidad de obtener los mejores servicios y mejores prácticas, el **CNS-IPCYT** elaborará un diseño de la arquitectura del servicio de seguridad considerando los elementos primordiales para proporcionar la confidencialidad, integridad, y disponibilidad de los activos tecnológicos de TI y comunicaciones del IMSS.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

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

El diseño de la arquitectura tecnológica integral estará conformado componentes de seguridad y un Centro de Operación de Seguridad (SOC), que rigen a los elementos tecnológicos de forma congruente para que el IMSS tenga un mayor beneficio y garantía en términos de seguridad de la información.

La arquitectura propuesta estará compuesta al menos, por los siguientes componentes:

- Firewall.
- DDoS.
- Redes Privadas Virtuales.
- Filtrado de Contenido Web.
- AntiSPAM.
- Web Application Firewall (WAF).
- Database Firewall.
- Centro de Operación de la Seguridad (SOC)

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

3.3.1.2. PRUEBAS Y VALIDACIÓN

El IMSS requiere un servicio de pruebas y validación mediante un área independiente de la operación del servicio de seguridad, a fin de garantizar las mejores prácticas y el buen funcionamiento de los servicios tecnológicos.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

El **CNS-IPCYT** del servicio integrará un área independiente a la que instala y opera el servicio de seguridad cuya función será la de ser un punto calidad de los servicios cuyo objetivo será validar que los mismos cumplan con los requerimientos y niveles de servicio solicitados por el **IMSS**.

El **IMSS** solicitara la realización de pruebas a las diferentes arquitecturas del servicio a fin de revisar que los diferentes componentes tecnológicos de los servicios de seguridad operen bajo las mejores prácticas de la gestión para las tecnologías de la información y telecomunicaciones.

3.3.1.3. ANÁLISIS DE VULNERABILIDADES

El **IMSS** requiere de un servicio que permita ejecutar análisis técnicos especializados sobre los activos de infraestructura de procesamiento y redes que permitan identificar vulnerabilidades nuevas y conocidas.

El **CNS-IPCYT** cumplirá al menos con las siguientes funcionalidades operativas:

- Capacidad para integrarse al menos dos herramientas que permitan complementar los análisis de vulnerabilidad ejecutados.
- Capacidad para identificar los servicios a analizar incluyendo el número de equipos involucrados y la versión de las plataformas de los sistemas.
- Identificación de vulnerabilidades documentadas en organismos internacionales como el CVE (Common Vulnerability Exposures).
- Identificación de configuraciones por omisión.
- Capacidad para elaborar un reporte técnico y ejecutivo donde se describa un riesgo asociado a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Capacidad para integrar un proceso-procedimiento de implementación de las medidas de remediación y recomendaciones realizadas, así como el integrar soporte técnico en la solución de los problemas presentados.
- Se dispondrá un número ilimitado de eventos para realizar procesos de análisis de vulnerabilidades bajo demanda conforme a las necesidades operativas.
- Capacidad para determinar el grado de vulnerabilidades ante técnicas de ataque como:
  - SQL Inyection.
  - Cross Site Scripting.
  - Cross Site Request Forgery.
  - Sensitive Data Exposure.
  - Security Misconfiguration.
  - Broken Authentication and Session Management.

3.3.1.4. PRUEBAS DE PENETRACIÓN.

El **IMSS** requiere de un servicio que permita realizar unas series de pruebas de penetración sobre la infraestructura con el fin de buscar fallas o debilidades en la seguridad de los sistemas. Todas las pruebas de penetración deberán ser realizadas con herramientas especializadas, así como por ingenieros calificados.

El **CNS-IPCYT** del servicio cumplirá con al menos las siguientes funcionalidades operativas:

- Identificación de los servicios o activos de información que se analizarán, incluyendo el número de los equipos involucrados y versión de las plataformas.
- Identificación de vulnerabilidades y malas prácticas de configuración.
- Explotación vulnerabilidades a los sistemas mediante las debilidades de seguridad detectadas.
- Evaluación de vulnerabilidades de al menos los siguientes rubros:
  - Autenticación y autorización.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Intentos ilimitados de inicio de sesión.
- Insuficiente autenticación.
- Insuficiente autorización.
- Gestión de Sesión.
  - Predicción de sesión o trabajo.
  - Secuestro de sesión.
  - Reproducir sesión.
  - Expiración de sesión insuficiente.
- Inyección de Código.
  - Inyección de comandos al sistema operativo.
  - Inyección de SQL.
  - Cross Site Scripting.
  - Inyección LDAP.
  - Inyección HTML.
  - Parameter Tampering.
  - Coockie Poisoning.
  - Hidden Field Manipulation.
- Criptografía.
  - Fortaleza del algoritmo.
  - Gestión de llaves.
- Ataques lógicos.
  - Abuso de funcionalidades.
  - Input Field Validation Checking.
- Protección de Datos.
  - Transporte.
  - Almacenamiento.
- Divulgación de información.
  - Indexado de directorio.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Path Transversal.
- Manejo inseguro de errores.
- Comentarios HTML.

3.3.1.5. ANÁLISIS FORENSE.

El **IMSS** requiere un servicio de análisis de incidentes de seguridad para determinar y documentar en que consistió el evento a través de la integración de registros o bitácoras que permitan obtener indicios de incidentes y su relación en el tiempo.

El **CNS-IPCYT** del servicio cumplirá con al menos las siguientes funcionalidades operativas:

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

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.3.1.6. CORRELACIÓN DE EVENTOS.

El **IMSS** requiere de un servicio de seguridad que maneje, analice y explote las bitácoras de los dispositivos de seguridad con la finalidad de conocer exactamente qué pasa en distintos puntos de la red de forma centralizada y eliminar falsos positivos generados. Se deberá de contar con una solución tecnológica para la administración de eventos e información de seguridad necesaria para el monitoreo, análisis, administración y reporte de eventos de seguridad de la información, que tengan como resultado proveer los mecanismos de identificación de incidentes y riesgos potenciales en la infraestructura y servicios tecnológicos del **IMSS**, entre los que se mencionan de manera enunciativa mas no limitativa, aplicaciones, servidores, equipos de comunicación, base de datos, con el fin de detectarlos, clasificarlos y tomas decisiones oportunas ante ellos.

La infraestructura propuesta será nueva, de última generación y dedicada exclusivamente para las necesidades del **IMSS**, y cumplirá con las siguientes especificaciones técnicas mínimas.

Cumplirá con al menos las siguientes funcionalidades operativas:

- Capacidad para recolectar datos de todas las aplicaciones o dispositivos que tengan una fuente de eventos necesarios para la organización, siendo esto a través de desarrollo predefinido del fabricante o con desarrollos personalizados ejecutados por el administrador del servicio.
- Capacidad para almacenar la información tal y como fue recibida del dispositivo o aplicaciones (eventos en crudo) para efectos de auditoria y análisis forense, la solución generará una firma o "checksum" de los eventos recibidos para garantizar la integridad y mantener la cadena de custodia.
- Permitirá la detección automática de fuentes de eventos recolectados a través del protocolo syslog, el cual puede ser enviado vía UDP, TCP o SSL/TLS.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Capacidad de permitir el filtrar eventos por cualquier campo de registro, que son los atributos donde se almacena la información recolectada por la herramienta de las fuentes de eventos.
- Contará con lógica de taxonomía a nivel de recolección de eventos, y que permitirá definir y modificar la misma con base a los eventos auditados.
- Capacidad para detectar automáticamente la desconexión un conector de integración a través del envío de señales de comunicación para el aseguramiento de la continuidad operativa ("keepalive").
- Capacidad para integrarse con los sistemas de detección y prevención de intrusos y los de administración de vulnerabilidades (VM).
- Contar con la capacidad de emitir notificaciones a partir de eventos y datos recopilados a través de mecanismos como SMTP, SNMP, y SYSLOG.
- Correlacionar eventos en tiempo real, es decir, que la información de los eventos sobre los que se está basando deberá venir del flujo del bus de mensajes.
- Capacidad para definir reglas de correlación con diferentes niveles de complejidad, partiendo de las basadas en patrones, hasta reglas basadas en periodos de tiempo, anidadas, causas/efecto, y secuenciales.
- El módulo de creación de reglas de correlación tendrá la capacidad de seleccionar eventos para hacer las reglas, así como de seleccionar campos del mismo para ser incluidos en la regla a través de mecanismos como "Drag and Drop".
- Contar con la capacidad de probar las reglas antes de ser implementadas en el motor de correlación.
- Comprimirá los datos almacenados al menos con una relación de 10 a 1.
- Contará con mecanismos de monitoreo de la integridad local y archivada.
- Capacidad para soportar de forma nativa la integración con soluciones de almacenamiento en red como SAN, NAS, NFS, o CIFS.
- Contará con una suscripción de boletines de seguridad más importantes del mercado para así identificar las vulnerabilidades conocidas, correlacionando la

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

información de herramientas de administración de vulnerabilidades con los eventos recolectados lo que permitirá automatizar su detección.

3.3.1.7. BORRADO SEGURO DE DATOS

Se realizará el borrado seguro de información en servidores, equipos de centro de datos, discos duros externos, y otras unidades de almacenamiento que imposibilite, ante cualquier intento o medio, la recuperación de la información borrada y permita la generación de un certificado que respalde la ejecución de borrado, esto debe ser totalmente automatizado y gestionado centralmente.

El **CNS-IPCYT** cumplirá con al menos las siguientes funcionalidades operativas:

- Permitirá realizar borrados completos en servidores derivados de sustitución de equipos, migraciones tecnológicas, o retiro por finalización de contrato.
- Asegurará que los datos no puedan ser recuperados, basándose en al menos los siguientes estándares internacionales:
  - HMG, Infosec Standard 5 (Baseline and Enhanced).
  - OPNAVINS5239.1
  - Extended NIST800-88.
  - DoD5220.22-M.
- Borrado de discos duros IDE/ATA, SCSI, SAS, USB, SATA, Fiberchannel, y Firewire de cualquier tamaño.
- Brindará la destrucción local y remota en múltiples dispositivos de almacenamiento.
- Posibilitará el desmontaje RAID (SCSI).
- Permitirá el borrado y detección de zonas bloqueadas/ocultas (DCO, HPA).
- Generará certificados de borrado infalsificables que ofrezcan protección ante cualquier instancia legal en donde se incluya el resultado el proceso de borrado, fecha, hora, los datos del equipo, el detalle del HD borrado.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Emitirá una firma electrónica para la autenticación de la integridad del reporte de sanitización emitido por el software de borrado.
- La solución podrá ejecutarse sin importar de que sistema operativo se trata.
- El reporte que genera la solución será exportado a un medio de almacenamiento como USB o disco duro.

3.3.1.8. SERVICIO DE SEGURIDAD PERIMETRAL PARA ENLACES DE BANDA ANCHA

El IMSS requiere un servicio que permita proporcionar la infraestructura que brinde seguridad perimètral para enlace de Banda Ancha, a través de los cuales se establece la transferencia de información entre diferentes unidades médicas y administrativas del IMSS.

El servicio de Seguridad perimetral para enlaces de banda ancha se entregará en dos modalidades:

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

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

- Contará un servicio de IPS.
- Contará con puertos de cobre Rj45
- Será un dispositivo de nivel empresarial.
- Será un dispositivo multifuncional, es decir integrar las funcionalidades descritas a continuación:
  - Firewall
  - IPS
  - Filtrado de Contenido
  - Detección y control de amenazas y programas maliciosos.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Contará con una consola de administración integrada accesible vía remota.
- Contará con doble fuente de poder.
- Garantizará técnicamente la seguridad de datos.
- Será compatible con direccionamiento IPv4 e IPv6
- Contará con la capacidad de manejo de VLANS.
- Podrá operar de manera transparente como un dispositivo de capa 2 y como un dispositivo de capa 3.
- Operará en alta disponibilidad tomado en cuenta los siguientes esquemas:
  - Modo Ruteo en capa 3 Activo/Activo
  - Modo Ruteo en capa 3 Activo/Pasivo
- Incluirá la capacidad de generar túneles VPN a través de protocolos IPSEC.
- Podrá aplicar QoS (Quality of Service) para priorizar tráfico de datos y/o video.
- Podrá crear políticas para usuarios y para grupos.
- Podrá identificar, permitir, bloquear o limitar el uso de aplicaciones independientemente del puerto.
- Permitirá el escaneo
- Contará con la administración centralizada de acceso a usuarios, a los recursos del **IMSS** y aplicaciones en Internet.
- permitir la conexión a las aplicaciones del **IMSS** a través de dispositivos móviles.

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

- contar un servicio de IPS.

- Deberá contar con puertos de cobre Rj45
- Deberá ser un dispositivo de nivel empresarial.
- Deberá ser un dispositivo multifuncional, es decir integrar las funcionalidades descritas a continuación:

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Firewall
- IPS
- Filtrado de Contenido
- Detección y control de amenazas y programas maliciosos.

- Contará con una consola de administración integrada accesible vía remota.
- Contará con doble fuente de poder.
- Garantizará técnicamente la seguridad de datos.
- Será compatible con direccionamiento IPv4 e IPv6
- Contará con la capacidad de manejo de VLANS.
- Podrá operar de manera transparente como un dispositivo de capa 2 y como un dispositivo de capa 3.
- Operará en alta disponibilidad tomado en cuenta los siguientes esquemas:
  - Modo Ruteo en capa 3 Activo/Activo
  - Modo Ruteo en capa 3 Activo/Pasivo
- Incluirá la capacidad de generar túneles VPN a través de protocolos IPSEC.
- Podrá aplicar QoS (Quality of Service) para priorizar tráfico de datos y/o video.
- Podrá crear políticas para usuarios y para grupos.
- Podrá identificar, permitir, bloquear o limitar el uso de aplicaciones independientemente del puerto.
- Permitirá el escaneo
- Contará con la administración centralizada de acceso a usuarios, a los recursos del **IMSS** y aplicaciones en Internet.
- Permitirá la conexión a las aplicaciones del **IMSS** a través de dispositivos móviles.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.3.1.9. SOPORTE PARA LA OPERACIÓN DE LA SEGURIDAD DE LA NUBE IMSS

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

- El SOC del **CNS-IPCYT** se ubica dentro del territorio mexicano (A fin de que se encuentre dentro de jurisdicción de las leyes mexicanas).
- Cuenta con un mecanismo que garantice la continuidad de la operación frente a contingencias.
- Operación 7x24x365 días durante la vigencia del contrato.
- Personal en sitio y remoto altamente calificado con las credenciales requeridas para la administración y monitoreo de los componentes que integran la solución.
- Operación de un centro de datos alterno ubicado dentro del territorio nacional.
- 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 de 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

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

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.
- Revisiones continuas de la operación del SOC, que permitan establecer mejora en los procesos, procedimientos y controles de seguridad.
- Servicio de correlación de eventos de seguridad y administración de bitácoras.
- Equipo de 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, intermitencia y /o perdida 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 Servicios apegada a ITILv3

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

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

- Numero directo de las instalaciones del SOC.
- Un numero 01 800 sin costo.
- Correo electrónico.

El personal del **CNS-IPCYT** cuenta con la experiencia probada en las áreas de tecnología y de seguridad de la información que se indica:

- Currículum Vitae de todo el personal donde se indica lo siguiente:
  - Experiencia profesional: Bajo este rubro se considerarán todos los cargos que cada integrante haya desempeñado.
  - Experiencia en proyectos de su especialidad.
  - Estudios: Bajo este rubro se anotarán todos los estudios en materia de seguridad de la información.
  - Incluir la estructura del grupo de trabajo, indicando por cada perfil la responsabilidades y competencias
  - El **IMSS** 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 contendrá 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.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.3.1.10. ADMINISTRACIÓN Y SOPORTE DE COMPONENTES DE SEGURIDAD

3.3.1.10.1. FIREWALL

El **IMSS** requiere de la seguridad y protección de control de acceso, bloqueo contra ataques dirigidos a las aplicaciones e inspección sobre los paquetes a nivel de aplicación para identificar patrones de tráfico anómalo. La infraestructura propuesta será nueva de última generación y dedicada exclusivamente para las necesidades del **IMSS** y cumplirá el **CNS-IPCYT** con las siguientes especificaciones mínimas:

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los Firewalls en la arquitectura de seguridad y comunicaciones.
- Habilitar esquema de alta disponibilidad.
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en las zonas del centro de datos correspondiente, o en su caso, donde le sea solicitado por el **IMSS.**
- Acordar con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware y software que integran el servicio sin ningún control de cambios autorizados por este último.
- Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Asegurar que el equipo propuesto cuente con la última versión estable, validad 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 **IMSS.**

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Permitir únicamente el tráfico definido por el **IMSS** 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 **IMSS**.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** 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 las 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 este caso de que el desempeño de la tecnología que soporta el servicio deberá realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades.

3.3.1.10.2. ANTI-DENEGACIÓN DE SERVICIOS (DDOS)

El **IMSS** 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

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

solución propuesta será nueva, de última generación y dedicada exclusivamente para las necesidades del **IMSS** y cumplirá con las siguientes especificaciones técnicas mínimas:

- El **CNS-IPCYT** definirá en conjunto con el **IMSS** la estrategia de habilitación de los equipos de Anti-denegación de Servicios (DDoS) en la arquitectura de seguridad y comunicaciones.
- El **CNS-IPCYT** habilitará esquema de Alta Disponibilidad (HA por sus siglas en ingles).
- El **CNS-IPCYT** 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 **IMSS**.
- El **CNS-IPCYT** acordará con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes hardware/software que componen el servicio sin un control autorizado por este último.
- El **CNS-IPCYT** integrará cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- El **CNS-IPCYT** asegurará que la solución propuesta contará con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.
- El **CNS-IPCYT** podrá prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- El **CNS-IPCYT** atenderá todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- El **CNS-IPCYT** 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:

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

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

En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el **CNS-IPCYT** realizará las adecuaciones necesarias para el correcto funcionamiento de la solución.

3.3.1.10.3. REDES VIRTUALES PRIVADAS (VPN).

El **IMSS** requiere del Servicio de Interconexión a través de Internet que permita establecer comunicación desde localidades remotas para la transferencia de información a través de un canal cifrado.

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los equipos para Redes privadas Virtuales – VPN en la arquitectura de seguridad y comunicaciones.
- Habilitar el esquema de Alta Disponibilidad (HA por sus siglas en ingles).
- Llevar a cabo todas las tareas necesarias para la Instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde lo sea solicitado el **IMSS**.
- Acordar con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes hardware/software que componen el servicio sin un control de cambios autorizado por este último.
- 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.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- Gestionar el alta de accesos remotos debida y previamente autorizados por el **IMSS** a través de los mecanismos y personal que para ellos designe este último.
- Solicitar de manera semanal la lista de usuarios dados de baja por la organización y proceder a la deshabilitación de sus accesos remotos de manera inmediata.
- Reportar bajo demanda la lista de usuarios y entidades (terceros) que cuentan con acceso remoto VPN C2S – S2S.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** 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 las soluciones de Prevención de Intrusos relacionados para al menos:
    - Cumplir las políticas de reglas de acceso a la Información.
    - Notificar sobre las actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución, configuradas para las cuentas de usuario o servicios con terceros.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el **CNS-IPCYT** deberá realizar solución de componentes tecnológicos por otros de igual o mejor características/funcionalidades.

3.3.1.10.4. FILTRADO DE CONTENIDO WEB.

El **IMSS** requiere del servicio de filtrado de contenido Web mediante políticas de acceso que permita controlar y filtrar la utilización del servicio de acceso a Internet, en función de roles y perfiles. La solución propuesta será nueva, de última generación y dedicada

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

exclusivamente para las necesidades del **IMSS** y cumplirá con las siguientes especificaciones técnicas mínimas:

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los equipos de Filtrado de Contenido Web en la arquitectura de seguridad y comunicaciones.
- Habilitar esquema de Alta Disponibilidad (HA por sus siglas en inglés).
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el **IMSS**.
- Acordar con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último,
- Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante. Siempre y cuando esté autorizado por el **IMSS**.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Filtrado de Contenido de Correo relacionados con al menos:
  - Cumplir las políticas de reglas de acceso a la información.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habilitadas en la solución. configuradas para las cuentas de usuario.

- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución de Filtrado de Contenido Web, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

- Acordar con el **IMSS** el tipo de implementación que se integrará para el uso de los servicios (modo implícito o explicito), y en su caso, podrá solicitar modificaciones al uso del mismo conforme las necesidades operativas así lo demanden.

3.3.1.10.5. ANTISPAM

El **IMSS** requiere del servicio de analizar correos electrónicos de entrada y salida con el objetivo de bloquear amenazas de spam, malware, phishing, amenaza persistente avanzada (Advanced Persistent Threat APT's), reputación de URLs embebidas en los correos. La solución propuesta será nueva, de última generación y dedicada exclusivamente para las necesidades del **IMSS** y cumplirá con las siguientes especificaciones-técnicas mínimas:

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los equipos de Filtrado de Contenido de Correo electrónico (Antispam) en la arquitectura de seguridad y comunicaciones.
- Habilitar esquema de Alta Disponibilidad (HA por sus siglas en ingles).
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el **IMSS**.
- Acordar con el personal del **IMSS** 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.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante. Siempre y cuando esté autorizado por el **IMSS**.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- Conocer y entender las políticas actuales de seguridad del **IMSS**, particularmente aquellas relacionadas con el manejo de información, las cuales serán entregadas en las Mesas de Trabajo correspondientes por parte del personal del **IMSS**.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Filtrado de contenido de Correo relacionados con al menos:

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

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea adecuado, el **CNS-IPCYT** realizará la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

3.3.1.10.6. ANTIMALWARE

El **IMSS** requiere de un servicio de detección y protección contra amenazas avanzadas en la red interna. La solución propuesta será nueva, de última generación y dedicada exclusivamente para las necesidades del **IMSS** y cumplirá con las siguientes especificaciones técnicas mínimas:

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los equipos de Antimalware en la arquitectura de seguridad y comunicaciones.
- Habilitar esquema de Alta Disponibilidad (HA por sus siglas en ingles).
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el **IMSS**.
- Acordar con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.
- Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

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

  - Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Antimalware relacionados para al menos.

  - Cumplimiento de las políticas de uso de información implantadas en la solución.

  - Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habitadas en la solución, configuradas para el tráfico externo y/o interno.

  - Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el **CNS-IPCYT** realizará la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

3.3.1.10.7. FIREWALL ESPECIALIZADO EN SERVICIOS WEB (WAF).

El **IMSS** requiere del servicio de protección, prevención y control de ataques para aplicativos webs expuestos en Internet. La infraestructura propuesta deberá ser nueva, de última generación y dedicada exclusivamente para las necesidades del **IMSS** y deberá cumplir con las siguientes especificaciones técnicas mínimas:

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los equipos de Firewall Especializado en Servicios Web (WAF) en la arquitectura de seguridad y comunicaciones.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Habilitar esquema de Alta Disponibilidad (HA por sus siglas en ingles).
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el IMSS.
- Acordar con el personal del IMSS todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.
- Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del IMSS.
- Revisar y validar en conjunto con el IMSS los requerimientos de protección, inspección de contenido http o https y de seguridad de aplicativos webs tal y como sea solicitado.
- Aprovisionar nuevos servicios aplicativos que requieran la protección a través del WAF, conforme el IMSS lo necesite.
- 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 IMSS 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.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificación sobre actividades sospechosas relacionadas con la violación de las políticas habitadas en la solución, configuradas para los servicios web públicos y/o privados.
- Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el **CNS-IPCYT** realizará la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

3.3.1.10.8. FIREWALL ESPECIALIZADO DE BASE DE DATOS.

El **IMSS** requiere del servicio de protección a las instancias de base de datos en tiempo real, así como el monitoreo del tráfico de base de datos con la finalidad de realizar la detección de ataques avanzados. La solución propuesta será nueva, de última generación y dedicada exclusivamente para las necesidades del **IMSS** y cumplirá con las siguientes especificaciones técnicas mínimas:

- Definir en conjunto con el **IMSS** la estrategia de habilitación de los equipos de Firewall Especializado en Base de Datos (DBF) en la arquitectura de seguridad y comunicaciones.
- Habilitar esquema de Alta Disponibilidad (HA por sus siglas en ingles).
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona del Centro de Datos correspondiente, o en su caso, donde le sea solicitado por el **IMSS**.
- Acordar con el personal del **IMSS** todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

cambios a los componentes de hardware/software que componen el servicio sin un control de cambios autorizado por este último.

- Integrar cada dispositivo hacia su respectiva consola de administración, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Asegurar que el equipo propuesto cuente con la última versión estable, validada, liberada y recomendada del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el fabricante.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del **IMSS**.
- El **CNS-IPCYT** atenderá todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **IMSS** genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- El **CNS-IPCYT** emitirá alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Firewall Especializado en Base de Datos (DBF) 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 habitadas en la solución, configuradas para los servicios de base de datos privadas.

    - Notificar todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la solución, efectuando la contención de las mismas haciendo uso de las bondades de la propia tecnología.

- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el **CNS-IPCYT** realizará la sustitución de componentes tecnológicos por otros de igual o mejor características/funcionalidad.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.3.2. SERVICIO DE ADMINISTRACIÓN DE RIESGOS TECNOLÓGICOS, (PROCESOS ASI Y OPEC)

El **CNS-IPCYT** apoyará al **IMSS** en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado al MAAGTICSI y basado en el estándar ISO 27001, que permitirá emitir directivas en materia de seguridad de la información a las áreas de TI y a los terceros que soportan la operación de TI.

El **CNS-IPCYT** del servicio cumplirá con al menos las siguientes funcionalidades operativas:

- Planear.
- Transferencia tecnológica Inicial – Curso "Inducción a la norma 27001:2013" Curso Introductorio que permite al participante:
  - Conocer la estructura de la norma ISO/IEC 27001:2013.
  - Interpretar los requisitos solicitados para el cumplimiento de la norma.
  - Conocer las etapas para la implementación de un SGSI.
- Generación de Directivas de Seguridad, manual de políticas de seguridad de la información:
  - Basadas en los dominios que establece la norma ISO 27001.
  - Alineados a los procesos de seguridad ASI y OPEC del MAAGTICSI.
  - Enfocadas a las áreas de TI y a los terceros que proveen servicios de TI al **IMSS**, considerando como alcance el catálogo de Infraestructuras Criticas del **IMSS**.
- Identificación y valuación de activos (Relacionado al catálogo de Infraestructuras Criticas) del proceso involucrado en el Sistema de Seguridad de la Información. La metodología contempla los siguientes puntos:

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

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

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

- Identificación y aplicabilidad de los requerimientos internos y externos.
- Selección de los objetivos control y controles para el tratamiento de los riesgos
- Verificación de requerimientos contractuales y legales.
- Identificación de los requerimientos internos y externos.
- Validación de aplicabilidad de los requerimientos.
- Formato para la autorización para implantar y operar el Sistema de Gestión de Seguridad de la Información.
- Preparación de la Declaración de Aplicabilidad.
- Documentar los objetivos de control y los controles elegidos y la justificación de su elección.
- Documentar los controles actualmente implementados.
- Documentar la exclusión de controles y la justificación de su exclusión.
- Implementar y opera en el Sistema de Gestión de Seguridad de la Información.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Análisis de Riesgos de Seguridad de la Información.
- Realización del Análisis de Riesgo con base en lo definido en el Servicio de Gestión de Riesgos de Seguridad.
- Generación del Plan de Tratamiento de Riesgos. La metodología contempla los siguientes puntos:
  - Identificación de las acciones a realizar por parte de la Organización y su Administración.
  - Identificación de los recursos necesarios y prioridades.
  - Identificación de las responsabilidades para administrar los Riesgos de Seguridad de la Información.
- Aplicación del Plan de Tratamiento de Riesgos. La metodología contempla los siguientes puntos:
  - Asignación de los roles y responsabilidades en la implantación de los controles relativos apersonas, procesos y tecnología involucrados en la mitigación de los riegos.
  - Actualización de documentación. Alineada a los requisitos establecidos en el proceso ASI y OPEC de MAAGTICSI.
  - Afinación de políticas y procedimientos de seguridad existentes.
  - Definición del proceso de reporte y atención de incidentes de seguridad (ERISC).
- Propuestas de implementación de los controles seleccionados, la metodología contempla los siguientes puntos:
  - Control de Accesos.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Monitoreo de Cuentas.
- Definición del proceso de continuidad del negocio.
- Implantación de los roles y responsabilidades definidas para el Sistema de Gestión de Seguridad de la Información.
- Controles de Seguridad en la Infraestructura Tecnológica de acuerdo a lo definido en el alcance.

➢ Administración del cambio cultural. La metodología contempla los siguientes puntos:

- Desarrollo de un programa de concientización con usuarios y operadores s del Sistema de Gestión de Seguridad de la Información.
- Determinación de las necesidades de Transferencia tecnológica para el personal que administre el Sistema de Gestión de Seguridad de la Información.
- Apoyo en la Transferencia tecnológica relativa a temas de seguridad de la información.
- Manual de Gestión de Seguridad de la Información. Se documentará un manual que contiene las referencias de la documentación generada en esta fase para dar trazabilidad al de las cláusulas de la norma.
- Monitorear y Revisar el Sistema de Gestión de Seguridad la Información.

➢ Revisiones gerenciales. La metodología contempla los siguientes puntos:

- Los dueños de procesos deben hacer una revisión al sistema de gestión de seguridad la información a fin de verificar que los objetivos del Sistema de Gestión de Seguridad de la Información están alineados a los objetivos de

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

negocio en materia de seguridad de la información y que garantizan el adecuado manejo de los riesgos existentes.

- El **CNS-IPCYT** generara el procedimiento de revisiones Gerenciales.
- El **CNS-IPCYT** propondrá los formatos requeridos para llevar acabo las revisiones.

➢ Auditorías Internas. La metodología contempla lo siguiente:

- Apoyo en la generación del plan de auditorías internas a las áreas de TI y los terceros que proveen servicios de TI al **IMSS**.
- Definición de los formatos requeridos para llevar a cabo las auditorias.
- Aplicación de una auditoría interna al Sistema de Gestión de Seguridad de la Información para verificar el cumplimiento con el estándar ISO/IEC 27001:2013 y a los procesos de seguridad ASI y OPEC del MAAGTICSI.
- Mantener y mejorar el Sistema de Gestión de Seguridad de la Información

➢ Implementación de mejoras. Contempla los siguientes puntos:

- Priorización de las acciones correctivas y no conformidades identificadas en las revisiones gerenciales, revisiones independientes, auditorías internas y revisiones técnicas.
- Identificación de los responsables de llevar a cabo las mejoras por parte de la organización.
- El **IMSS** definirá las fechas compromiso para la terminación de las mejoras, únicamente para el seguimiento interno.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Tomar acciones correctivas y en las no conformidades. Contempla los siguientes puntos:
  - Apoyo en la definición del procedimiento para realizar acciones correctivas y no conformidades derivadas de las auditorías.
  - Definición del formato para el llenado de acciones correctivas y no conformidades.
  - Coordinación de la ejecución de las acciones correctivas ya definidas y en su caso las no conformidades que se identifiquen.
- Comunicar los resultados de las acciones tomadas. Contemplar el siguiente punto:
  - Apoyo en la programación de reuniones de seguimiento al Sistema de Gestión de Seguridad de la Información para dar a conocer el alcance de las acciones correctivas y no conformidades realizadas y verificar su apego a los requerimientos de los dueños de la información y los involucrados en los procesos del **IMSS.**

3.3.3. SERVICIO DE ANÁLISIS DE RIESGOS (PROCESOS ASI Y OPEC), APÉNDICE SEGURIDAD

Identificar, evaluar y manejar los riesgos de la seguridad de la información, utilizando técnicas estadísticas, información histórica, fuentes de información especializada y otras que permitan, determinar la exposición a diferentes escenarios de riesgo, probabilidad e impacto, así como la recomendaciones y líneas de acción, que permita alcanzar un nivel de seguridad aceptable a un costo razonable enfocado al catálogo de infraestructura críticas del **IMSS.** El **CNS-IPCYT** cumplirá cumplir con las siguientes funcionalidades operativas:

- Contexto

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Recopilar información sobre las operaciones del **IMSS**, las relaciones entre los procesos de negocio, procesos y recursos de tecnológica, las dependencias entre estos, tomando en cuenta:

  a. Consideraciones generales del **IMSS**.

  b. Definición de criterios básicos para la ejecución del análisis.

  c. Definición del alcance del análisis.

  d. Definición del equipo de trabajo del **CNS-IPCYT** y del **IMSS** que participara en la ejecución del análisis.

- Valoración de Riesgos.

  - Utilizar la metodología basada en el proceso ASI del MAAGTICSI para la gestión de riesgos de la seguridad. La metodología contendrá:

    a. Identificación de activos, considerando como activos a los procesos, actividades, información, infraestructura, y gente.

    b. Identificación de vulnerabilidades.

    c. Identificación de amenazas.

    d. Escenarios de riesgo.

    e. Priorización del riesgo.

- Tratamiento de los riesgos.

  - Criterios para la atención del riesgo identificado y analizando varias opciones de tratamiento de las cuales se elegirá la que mejor balance Costo-Beneficio genere, considerando el resultado obtenido:

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

a. Evitar

b. Mitigar

c. Transferir

d. Aceptar

- Seguimiento y Mitigación de Riesgos.
  - Deberá dar seguimiento a los planes de tratamiento de riesgos conforme a lo siguiente:
    a. La generación de los planes de mitigación de riesgos.
    b. Identificación de los responsables de cada plan.
    c. Acompañamiento en la implementación de controles normativos.

3.3.4. ENTREGABLES DE ÚNICA OCASIÓN

Centro de Operaciones de Seguridad (SOC)

- Diseño físico y lógico de alto nivel con la descripción detallada de la arquitectura propuesta para habilitar los servicios de la solución de seguridad.
- Copia de los siguientes procesos de seguridad que tiene implementados en el "SOC":
  - Proceso de Administración y Control de Cambios.
  - Proceso de Disponibilidad.
  - Proceso de Administración de Vulnerabilidades.
  - Proceso de Atención y Respuesta a Incidentes.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Proceso de Mejora Continua.

- La matriz de escalamiento del servicio tanto técnico como jerárquica.
- Procesos de la Mesa de Servicio, que se indican a continuación:
  - Administración de incidentes.
  - Administración de problemas.
  - Administración de cambios y configuraciones.
  - Administración de liberaciones.
- Metodología para el proceso de administración de vulnerabilidades.
- Procedimientos de seguridad aplicados en el "SOC" para:
  - Manejo de alarmas.
  - Análisis y Correlación de Eventos de Segundad.
  - Atención y Respuesta a Incidentes de Seguridad.

3.3.5. ENTREGABLES PERIÓDICOS

El **CNS-IPCYT** generará de manera integrada un Entregable Mensual del Servicio de Seguridad, que incluya de manera enunciativa más no limitativa los siguientes conceptos:

3.3.5.1. 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.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Reporte de incidentes atendidos en los activos de infraestructura (firewall), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (firewall), incluyendo tiempos de solución.
- Reporte de promedio de tráfico de entrada/salida por cada DMZ asignada.
- Reporte del top diez (10) de los protocolos bloqueados.
- Reporte del top diez (10) de los protocolos permitidos.
- Repone de reglas de control de acceso más utilizadas.
- Reporte del top diez (10) de direcciones IP Publicas/Privadas con más consumo de ancho de banda.

3.3.5.2. ANTI-DENEGACIÓN DE SERVICIOS (DDOS)

- Reporte de la disponibilidad de los activos de infraestructura (AntiDDoS), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (AntiDDoS), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (AntiDDoS), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (AntiDDoS), incluyendo tiempos de solución.
- Reporte del top diez (10) de anomalías clasificadas por nivel de severidad.
- Reporte del top diez (10) de activos de infraestructura con mayor número de incidencias de tráfico anómalo (internos/externos).
- Reporte del top diez (10) de protocolos bloqueados.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.3.5.3. REDES PRIVADAS VIRTUALES – VPN

- Reporte de la disponibilidad de los activos de infraestructura (Concentrador VPN), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (Concentrado VPN), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (Concentrador VPN), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (Concentrador VPN), incluyendo tiempos de solución.
- Reporte del top diez (10) usuarios que se conectan a través de VPN C2S.
- Reporte del top diez (10) de servicios (direcciones 1P destino) que se conectan a través de VPN C2S y S2S.
- Reporte del top diez (10) de ancho de banda consumido por VPN S2S.

3.3.5.4. FILTRADO DE CONTENIDO WEB.

- Reporte de la disponibilidad de los activos de infraestructura (Filtrado de Contenido Web), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de infraestructura (Filtrado de Contenido Web), incluyendo tiempo de atención.
- Reporte de incidentes atendidos en los activos de infraestructura (Filtrado de Contenido Web), incluyendo tiempos de mitigación/remediación.
- Reporte de fallas atendidas en los activos de infraestructura (Filtrado de Contenido Web), incluyendo tiempos de solución.
- Reporte del top veinte (20) sitios web bloqueados.
- Reporte del top veinte (20) sitios web permitidos.
- Reporte del top veinte (20) categorías bloqueadas.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Reporte del top veinte (20) categorías permitidas.
- Reporte del top veinte (20) de IP/Usuarios con mayor navegación a Internet,
- Reporte del top veinte (20) de IP/Usuarios con mayor consumo de ancho de banda.

3.3.5.5. ANTISPAM.

- Reporte de la disponibilidad de los activos de infraestructura (Antispam), incluyendo, un análisis de la indisponibilidad de los dispositivos en los casos que se hayan presentado.
- Reporte de los controles de cambios en de los activos de Infraestructura (Antispam), incluyendo tiempo de atención.

3.3.6. ENTREGABLES BAJO DEMANDA.

El **CNS-IPCYT** generara bajo demanda los siguientes documentos y/o reportes, a solicitud del órgano de gobierno que señale el **IMSS**; y que incluyen de manera enunciativa más no limitativa los siguientes conceptos:

3.3.6.1. SERVICIOS DE CONTROL DE CALIDAD

3.3.6.1.1. ANÁLISIS DE VULNERABILIDADES

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades, detectadas por cada activo o grupo de activos de infraestructura Escaneados, así como el plan de mitigación propuesto.
- Archivos electrónicos (MS Excel) con la información fuente obtenida de las herramientas tecnológicas que se utilizaron para realizar los escaneos de vulnerabilidades.
- Reporte de los escaneos de vulnerabilidades realizados, indicando al menos: Activo(s) De infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja).

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.3.6.1.2. PRUEBAS DE PENETRACIÓN

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades, detectadas por cada activo o grupo de activos de infraestructura Verificados, así como el plan de mitigación propuesto.
- Archivos electrónicos (MS Excel) con la información fuente obtenida de las herramientas tecnológicas que se utilizaron para realizar las pruebas de penetración.
- Reporte de las pruebas de penetración realizadas, indicando al menos: Activo(s) De infraestructura o aplicativo relacionado, fecha de ejecución, direccionamiento IP, Vulnerabilidades detectadas (Alta, Media, Baja).

3.3.6.1.3. ANÁLISIS FORENSES

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle del análisis forense ejecutado por cada activo o grupo de activos de infraestructura verificados.

3.3.6.1.4. BORRADO SEGURO DE DATOS

- Reporte Técnico/Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro por cada activo o grupo de activos de infraestructura eliminados.
- Archivos electrónicos (HTML y PDF) con la información fuente obtenida de las herramientas tecnológicas que se utilizaron para realizar los borrados seguros de la información.
- Reporte mensual de los borrados seguros realizados, indicando al menos: Activo(s) de infraestructura, fecha de eliminación.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.3.6.1.5. ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

- Reporte ejecutivo en formato electrónico (MS Word, PDF) de la actividad de Análisis de Riesgos que incluya:
  - Identificación activos, considerando como activos a los procesos, actividades, información, infraestructura, y gente.
  - Identificación de vulnerabilidades.
  - Identificación de amenazas.
  - Escenarios de riesgo.
  - Priorización del riesgo.

3.3.6.1.6. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

- Reporte de actividades relacionadas con las solicitudes de implementación, Evaluación y/o Mejora del sistema de Gestión de Seguridad de la Información que incluya:
  - Transferencia tecnológica inicial
  - Generación de directivas de seguridad
  - Identificación y valuación de activos
  - Generación de la Declaración de Aplicabilidad
  - Generación del plan de tratamiento de riesgos
  - Propuestas de implementación de los controles

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Manual de Gestión de seguridad de la información

Los reportes y/o documentos anteriores deberán ser entregados en el formato y fecha que hayan sido acordados con el órgano de gobierno del **IMSS** que los haya solicitado y deberán ser integrados al Entregable Mensual del servicio de Seguridad) en el periodo que corresponda a su entrega, para la validación de los niveles de servicio que correspondan.

3.3.7. CONSIDERACIONES GENERALES PARA LA ENTREGA DE LOS SERVICIOS DE SEGURIDAD.

El **CNS-IPCYT** 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 **IMSS**.

- Contar con servicios de infraestructura regulados por niveles de servicio, que: implementen (instalen, migren, habiliten y pongan a punto) los componentes necesarios en los Centros de Datos del **IMSS**, 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 **IMSS**.
- Contar con servicios de seguridad de la información, que complementen el esquema de seguridad institucional de forma consistente y robusta. con el control,

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

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 **IMSS**, entendiendo que toda actualización o mejora debe ser consultada y aprobada por este último.
- Garantizar la operación. Licenciamiento, soporte técnico, mantenimiento correctivo y preventivo, así como el reemplazo de partes (por parte del fabricante del componente o de la solución), de los servicios propuestos, considerando la cantidad de unidades de licenciamiento como los dispositivos, los usuarios concurrentes. entre otros, conforme la naturaleza y características del servicio que dicha infraestructura y base instalada soportan.
- Integrar a los servicios de gestión, operación, soporte y mantenimiento provistos por su Centro de Operaciones de Seguridad (SOC) para los servicios ofrecidos, dando cumplimiento a las condiciones del presente contrato.
- Establecer Mesas de trabajo con el **IMSS**, 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 **IMSS** previo a la transición a la operación del servicio.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- 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 un número telefónico 01 800 para dar soporte a los usuarios del **IMSS**.
- 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 **IMSS** validar en cualquier momento los elementos que componen los diversos servicios.

3.4. UNIDAD INTEGRAL DE VIRTUALIZACIÓN RED HAT O COMPATIBLE.

El **CNS-IPCYT** entregará mediante los mecanismos, las herramientas, servicios virtuales y sus componentes, una plataforma de virtualización RHEV o compatible, que permita al **IMSS** desarrollar plenamente el despliegue de los componentes virtuales que integran esta solución, lo anterior deberá incluir al menos lo siguiente:

- ***Red Hat Enterprise Linux Smart Virtualization***
- ***Red Hat OpenShift Container Platform Standard, 2-Core o compatible.***
- ***Red Hat Ansible Automation Standard (100 Managed Nodes) o compatible***
- ***Red Hat CloudForms Premium (Managed Nodes: Physical (2 sockets) or Virtual (16), public cloud) o compatible.***

Imagen 1- Solución de Virtualización Red Hat

Referencia: https://www.redhat.com/cms/managed-files/vi-enterprise-linux-with-smart-virtualization-datasheet-f9339kc-201710-a4-es.pdf

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

La unidad integral de virtualización tendrá soporte durante la vigencia del contrato y la cual incluirá todos los componentes necesarios para su correcto funcionamiento.

Adicionalmente, el **CNS-IPCYT** incluirá dentro de su propuesta la instalación del software Red Hat Enterprise Linux por nodo solicitado por el **IMSS**. El cual estará funcionando de forma correcta y contemplará todos los componentes necesarios llámese de hardware y/o software sin costo adicional al **IMSS**. Lo anterior, será validado por el personal que este designe.

3.5. UNIDAD DE ALMACENAMIENTO DE OBJETOS SOBRE PLATAFORMA DE NUBE PÚBLICA

El **CNS-IPCYT** otorgara un esquema de consumo de almacenamiento de objetos en nube pública con la característica principal de ser escalable a las necesidades del **IMSS**.

El **CNS-IPCYT** brindara una solución integral que asegure la escalabilidad, garantizando la disponibilidad de los datos almacenados, seguridad y el rendimiento en el acceso a los mismos.

La solución propuesta por el **CNS-IPCYT** soportará diversos casos de uso, que, con el previo diseño de la infraestructura involucrada pueda ser compatible con los escenarios que el **IMSS** pueda proyectar. Como ejemplo de los escenarios que la plataforma debe ofrecer son: uso para sitios web, aplicaciones móviles, procesos de copia de seguridad y restauración, operaciones de archivado, aplicaciones empresariales. La solución propuesta por el **CNS-IPCYT** contará con características de administración fáciles de utilizar que permitan organizar los datos y configurar sofisticados controles de acceso. Así mismo, se ofrecerá una disponibilidad del 99,9999 %.

El **CNS-IPCYT** entregará uno de los siguientes esquemas, siendo limitativo a la ejecución de un esquema, pero con la posibilidad de escalar hasta el más demandante:

- Esquema 1:

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

a. Almacenamiento disponible: 500 TB
   - ✓ Cantidad de Peticiones PUT/COPY/POST/LIST soportadas: 1,000,000
   - ✓ Cantidad de Peticiones GET/SELECT/Other soportadas: 1,000,000

b. Transferencia de datos
   - ✓ Salida: 2 TB al mes
   - ✓ Entrada: 10 TB al mes

➢ Esquema 2:

a. Almacenamiento disponible: 750 TB
   - ✓ Cantidad de Peticiones PUT/COPY/POST/LIST soportadas: 3,000,000
   - ✓ Cantidad de Peticiones GET/SELECT/Other soportadas: 3,000,000

b. Transferencia de datos
   - ✓ Salida: 10 TB al mes
   - ✓ Entrada: 50 TB al mes

➢ Esquema 3:

a. Almacenamiento: 1 PB
   - ✓ Cantidad de Peticiones PUT/COPY/POST/LIST soportadas: 5,000,000
   - ✓ Cantidad de Peticiones GET/SELECT/Other soportadas: 5000000

b. Transferencia de datos
   - ✓ Salida: 20 TB al mes
   - ✓ Entrada: 100 TB al mes

➢ Esquema 4:

c. La modalidad de dicho esquema podrá ser la combinación de los esquemas anteriores o en su caso la incorporación de nuevas soluciones de almacenamiento de este tipo las cuales podrán estar vigentes durante la vigencia del contrato.

La solución propuesta por el **CNS-IPCYT** será la de **Amazon S3**, la cual permite utilizar los esquemas que se mencionan previamente.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

Imagen 2 - Solución de Amazon S3

Referencia: https://aws.amazon.com/es/s3/

3.6. UNIDAD INTEGRAL DE CONMUTACIÓN DE DATOS Y DE PROTECCIÓN CONTRA AMENAZAS Y DETECCIÓN DE INTRUSOS

Con la finalidad de obtener la mejor solución de seguridad de la información, el área independiente de punto de control de calidad elaborará el diseño de la arquitectura de seguridad, considerando los elementos necesarios para proporcionar la confidencialidad, integridad y disponibilidad de los activos de tecnologías de información y comunicaciones del **IMSS**. Esta estrategia permitirá consolidar la integración de servicios, funciones, sistemas e infraestructura tecnológica en busca de mayor eficiencia, productividad y economías de escala.

En lo referente a la administración y control de la seguridad informática se requiere el diseño de una arquitectura tecnológica integral que tenga par objetivo proveer infraestructura tecnológica que operen con altos niveles de disponibilidad y eficiencia. Bajo las mejores prácticas de gestión para las tecnologías de la información y comunicaciones.

Esta arquitectura tecnológica integral se conformará de diferentes plataformas específicas, que deberán trabajar en conjunto de forma transparente y segura, para que el **IMSS** obtenga el mayor beneficio en términos de seguridad de la información en el uso de la tecnología.

Adicionalmente, el **CNS-IPCYT** realizará los protocolos de pruebas, interoperabilidad y validación de todos los componentes que integran está solución teniendo un único punto

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

de control de calidad, el cual tiene como objetivo tiene realizar las validaciones correspondientes que permitan cumplir con lo solicitado en la presente propuesta.

El **CNS-IPCYT** en conjunto con el **IMSS** realizará las pruebas y validaciones a fin de dar certeza de que estos componentes se encuentran establecidos bajo las condiciones establecidas en la presente propuesta. La arquitectura tecnológica integral que fortalecerá la plataforma de seguridad de la información del **IMSS** se integrará de los siguientes elementos:

3.6.1. Unidad integral de Conmutación de Datos

La unidad de componente integral de conmutación de datos 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 y LAN to LAN, redireccionándolos hacia los destinos correspondientes.

El equipamiento propuesto para la red de área local en el Centro de Datos ofertado considerará e incluirá 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.

La solución considerará e incluirá toda la infraestructura y los insumos necesarios para brindar conectividad a las diferentes aplicaciones del **IMSS** y dispositivos de TICS que así lo requieran.

Contará con mecanismos de separación de tráfico para coadyuvar a una mejor administración de la infraestructura de TICS.

Mantendrá una alta disponibilidad para el intercambio ágil, rápido íntegro y confiable de la información entre los servicios del **IMSS** que estarán conectados.

Las características mínimas por incluir son:

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- El **CNS-IPCYT** podrá crear al menos una VLAN para lograr la extensión del direccionamiento LAN del **IMSS**, sin embargo, el **IMSS** 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 **CNS-IPCYT** podrá garantizar el flujo de tráfico entre todas las VLAN's que solicite el **IMSS**. Todas las VLAN's deberán ser implementadas con un ancho de banda de al menos 1 GB, por lo que el **CNS-IPCYT** deberá considerar el equipamiento necesario para lograrlo.
- El **CNS-IPCYT** podrá considerar que todas las VLAN´s deberán estar debidamente aisladas de otros clientes que tengan servicios en el Centro de Datos contratado actualmente por el **IMSS**, de forma que ningún paquete de datos que fluya sobre la o las VLAN's que se implementen para el **IMSS** viaje a través una VLAN de otro cliente; tampoco estará permitido que paquetes de datos de otros clientes del Posible **CNS-IPCYT** viajen a través de las VLAN's que se implementen para el **IMSS**.
- El **CNS-IPCYT** considerará e incluirá el transporte, la conmutación, así como el enrutamiento de paquetes, a conveniencia o solicitud del **IMSS**.
- Debido a que los servicios de red son la base de operación de todo servicio de TIC que se proporcione al **IMSS**, cualquier falla en los servicios de red, se considerará como una falla en los servicios que soportan la operación del **IMSS**, afectando la disponibilidad de las aplicaciones involucradas, lo que originará las sanciones correspondientes
- Los servicios de red descritos no representarán costos adicionales para el **IMSS**, pues se entiende que forman parte del servicio cotizado en un periodo mensual unitariamente al **IMSS**.
- El **IMSS** 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

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

redundancia en fuentes de poder y en su caso redundancia tarjetas controladoras o administradoras.

- El **IMSS** tiene el derecho de efectuar en cualquier momento y las veces que considere necesario, las inspecciones físicas en las instalaciones del **CNS-IPCYT**, con la finalidad de verificar el cumplimiento de lo solicitado.
- El **CNS-IPCYT** considerará e incluirá 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 **IMSS** intercambia de manera segura información con diversas Instituciones.
- El **CNS-IPCYT** integrará todo lo necesario para soportar la recepción de enlaces LAN to LAN (L2L), para generar la conectividad con terceros.

El **CNS-IPCYT** proporcionará una topología en alta disponibilidad para los Switches Core y los switches de acceso con velocidades de transmisión de 10Gbps. Lo anterior, nos permite proporcionar el ancho de banda necesario para el transporte de los datos, video y voz. La anterior, proporciona un esquema flexible de crecimiento con base en las necesidades del **IMSS**.

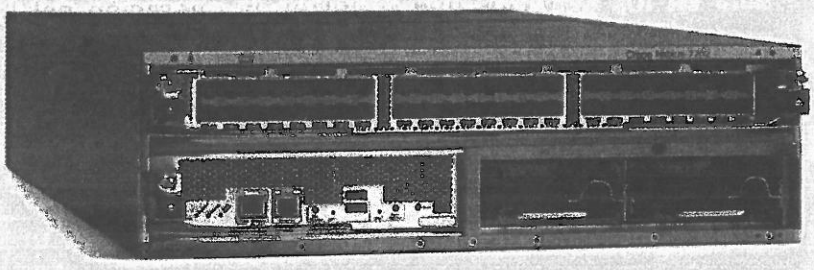


Imagen 3 - Solución de Red Cisco Nexus 7000

Referencia: https://www.cisco.com/c/en/us/products/switches/nexus-7000-series-switches/index.html

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.6.2. Unidad integral de firewalls de siguiente generación

El **IMSS** requiere el aprovisionamiento de la infraestructura que brinde seguridad perimetral, protección de control de acceso, bloqueo contra ataques dirigidos a las aplicaciones e inspección sobre los paquetes a nivel de aplicación que permita la identificación de patrones de tráfico anómalo.

El **CNS-IPCYT** en conjunto con el **IMSS** definirá en conjunto la estrategia de implementación de los firewalls que formarán parte de la arquitectura de seguridad y comunicaciones definida en la presente propuesta. La solución propuesta estará configurada bajo un esquema de alta disponibilidad.

El **CNS-IPCYT** llevará a cabo todas las tareas necesarias para la instalación del equipamiento y el cual se ubicará dentro de su centro de datos.

La solución propuesta estará configurada y funcionando en un esquema de alta disponibilidad siendo esta una solución de siguiente generación de propósito específico; es decir que el equipamiento propuesto deberá estar dedicada a las funcionalidades de firewall, IPS, visibilidad granular y control de aplicaciones y filtrado de contenido web.

Adicionalmente, La solución incluirá los componentes de hardware y software necesarios para su gestión a manera de poder administrar y monitorear los logs, manejo de imágenes de software, configuración de alertas y health check, etc. Esta solución controlará el acceso a la salida a internet, las zonas desmilitarizadas y proporcionará los mecanismos de protección contra amenazas persistentes, del dia zero, detección de intrusos y protección contra malware avanzado. Así mismo, permitirá la publicación segura de los aplicativos y sistemas que el **IMSS** designe.

El **CNS-IPCYT** incluirá el software (virtualización y sistema operativo) y hardware requerido para la correcta instalación de los componentes de gestión de la solución así mismo el **CNS-IPCYT** podrá instalar las aplicaciones que de acuerdo al dimensionamiento

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

puedan ser virtualizado en un mismo servidor, se incluirá todo los componentes necesarios para el correcto funcionamiento de la gestión de la solución de firewalls de siguiente generación; en cuanto a la conectividad del hardware (servidor), se incluirán al menos 2 Interfaces 100/1000 en cobre para la conexión a la red del centro de datos del CNS-IPCYT.

El equipamiento propuesto será nuevo, de última generación y dedicado para las necesidades del IMSS y cumplirá con las siguientes especificaciones técnicas mínimas de forma enunciativa más no limitativa:

CARACTERISTICA TECNICA	REQUERIMIENTO SOLICITADO	
Características Técnicas de Firewall	Desempeño de Firewall	39 Gbps
	Desempeño de prevención de amenazas	18 Gbps
	Desempeño IPSec VPN	16 Gbps.
	Conexiones por segundo	284,000
	Sesiones Concurrentes	8,000,000
	Configuración en alta disponibilidad	Activo/Activo Activo/Standby
	Modo de Operación en capa 3 (routing)	Incluido
	Soporte NAT	Incluido
	Soporte PAT	Incluido
	Conexiones incluidas VPN Site to Site	4000
	Conexiones incluidas VPN Client to Site	4000
Características de Nueva Generación (NGFW)	Inspección de al menos 1 000 distintas aplicaciones,	Incluido

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

	así como de 75,000 de micro aplicaciones	
	Utilización de Inspección Paquetes Profunda (DPI)	Soportado
	Detección y prevención de intrusos (IPS) Filtrado de contenido de la WEB Detección y control de virus Detección y control de amenazas y programas maliciosos Bloquea un rango de amenazas conocidas (como exploits, malware y spyware) a través de todos los puertos independientemente de las tácticas comunes de evasión de amenazas empleadas	Incluido
	Monitoreo centralizado que incluya el licenciamiento para permitir el reporteo, visualización de logs y eventos	Incluido
	Rango de Voltaje en línea	100 - 240V
	Voltaje Normal	100 - 240V

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

	Conectividad Eléctrica	Se deberá proporcionar los conectores hembra/macho y PDU´s de interconexión eléctrica necesarios.
Características de Enrutamiento	Policy-based routing	Incluido
	Multicast Routing	Incluido
	IGMP (v1, v2)	Incluido
Características Físicas	PIM SM	Incluido
Características Eléctricas Características de Interfaces	OSPF	Incluido
	Puertos Físicos 10GE (SFP+)	4 puertos incluidos SR
	Puertos de comunicación	Incluido jumper e interfaz física por puerto incluido
Características de Enrutamiento Características IPv6 Características de Administración y Monitoreo	Puertos Físicos 10/100/1000 Base-T	4 puertos incluidos
	Puerto Consola	Incluido
	Dual Stacking firewall	Incluido
	Generación de reporteo de firewall (top services, top sources, top destinations)	Incluido
Características de Reporteo	Generación de reporteo de IPS (Top Attackers, Top Blocked/Unblocked Signatures, Top Signatures)	Incluido

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

	Generación de reporteo de VPN (Top Bandwidth Users (SSL/IPsec)	Incluido
	WEBGUI Global	Incluido
	WEBGUI dedicado por firewall virtual	Incluido
Características IPv6	Monitoreo de las aplicaciones que cursan la red	Incluido
Características de Administración y Monitoreo Protección de Ataques Conocidos Características VPN	Monitoreo de la actividad web de usuarios en la red	Incluido
	Permita la generación de contraseña de acceso por firewall virtual	Incluido
	Visualización Número de sesiones en tiempo real por firewall virtual.	Incluido
	Visualización en Uso de CPU en tiempo real del firewall	Incluido
	Visualización de Actividad de eventos en consola en tiempo real por firewall virtual	Incluido
	Interfaz de administración por CLI en consola	Incluido
	Interfaz de administración	Incluido

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

	por CLI mediante SSH por firewall virtual.	
	Interfaz de administración por CLI mediante TELNET por firewall virtual	Incluido
	Administración por CLI de cada instancia de firewall virtual	Incluido
	Múltiples servidores de SYSLOG	Incluido
	Notificación por medio de correo electrónico	Incluido
	SNMPv2	Incluido
	SNMPv3	Incluido
	Logging Remoto	Incluido
	Monitoreo de Túneles VPN	Incluido
	Protección a ataques FLOOD	Incluido
	Protección a ataques fragmentados de ICMP	Incluido
	Protección a ataques de escaneo de puertos	Incluido
	Protección a ataques de Denegación de Servicio (DoS)	Incluido
	Protocolo de encripción 3DES	Incluido

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

	Protocolo de encripción AES	Incluido
	Autenticación MD5	Incluido
Protección de Ataques Conocidos	Autenticación SHA-1	Incluido
	Grupos DIFFIE HELLMAN	Incluido
	IPSEC NAT Transversal	Incluido
	Configuración Hub & Spoke en VPN Site to Site	Incluido
Certificaciones	SOC2. FIPS 140-2, Common Criteria, NCSC Foundation Grade Certification, ANSSI top-level certification.	incluido
Servicios Profesionales	Diseño (plan migración de las actuales configuraciones de seguridad), optimización, instalación, configuración y puesta en operación.	Incluido

El equipamiento propuesto de firewalls de siguiente generación es un Palo Alto Networks PA-5520, el cual será instalado, configurado y puesto en marcha por el **CNS-IPCYT**. Adicionalmente, el equipamiento estará configurado bajo un esquema de alta disponibilidad, lo cual permitirá incrementar los niveles de disponibilidad.

Imagen 4 - Solución de Firewalls de Siguiente Generación PA-5520.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

Referencia: https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall

3.6.3. Unidad Integral de firewall de aplicaciones web

EL CNS-IPCYT integrará una solución que contenga técnicas de detección y mitigación para frustrar los ciberataques más sofisticados y los detenga incluso antes de que lleguen a los servidores, este la solución aparece con un porcentaje mayor al 99.80% de eficacia en una comparativa (Web Application Firewall Comparative Analysis) de nss labs y es calificado como líder, dentro de su reporte anual, por la firma consultora y de investigación Gartner. La solución cumplirá de forma enunciativa, mas no limitativa con las características que a continuación se enlistan:

- La solución contará con un modo aprendizaje para rastrear cambios continuos dentro de las aplicaciones web del **IMSS**, deberá reconocer dichos cambios y simultáneamente protegerlas. La solución propuesta deberá soportar lo siguiente:
- La solución de firewall de aplicación web y el monitoreo de actividades para el firewall de inspección de archivos soportará el licenciamiento para la protección de aplicaciones web en paquetes de 10 aplicaciones web, los cuales podrán ser integrados de acuerdo a las necesidades del **IMSS**.
- Aprenderá los valores aceptables para los campos de ingreso de datos con base en el registro de la actividad.
- De los valores aprendidos, serán utilizados como la configuración inicial sobre la que se revisarán los datos ingresados en el modelo positivo de seguridad.
- En modo aprendizaje, aprenderá la estructura y elementos de la aplicación (directorios, url´s, parámetros, cookies) y el comportamiento esperado del usuario (longitud del valor esperado, caracteres aceptados, si el parámetro es de

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

sólo lectura o editable por el usuario) y esta información estará disponible para automatizar la configuración del modelo positivo de seguridad.

- La configuración aprendida será accesible y modificable para el administrador del dispositivo.
- La solución correlacionará múltiples eventos de seguridad para distinguir tráfico deseado del tráfico inadecuado.
- La solución permitirá la modificación de reglas de seguridad. Los administradores podrán definir reglas para el modelo de seguridad positivo o negativo y crearán reglas de correlación con múltiples criterios.
- Las políticas granulares para control de acceso o generación de alertas contarán con los siguientes criterios para la validación de la actividad en la aplicación Web. Los criterios podrán 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 el HTTP Request o el Response por parte del servidor Web
  - ✓ Tipo de archivo siendo transmitido en cualquier sentido
  - ✓ Host o dominio accedido
  - ✓ Métodos HTTP usados
  - ✓ Número de ocurrencias en intervalos de tiempo definidos
  - ✓ La existencia o contenido de cualquier Parámetro web
  - ✓ Por el protocolo usado, HTTP o HTTPS
  - ✓ IPs de origen y destino

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- ✓ Por la existencia o contenido de Cookies o el identificador de Sesión
- ✓ Response Code y Headers en el Response HTTP por parte del servidor Web
- ✓ Hora del Día
- ✓ Por usuario firmado en el aplicativo web
- ✓ User-Agent
- ✓ Referer-URL
- ✓ Tiempo de respuesta o tamaño de la respuesta HTTP

- ➢ La solución contará con el modo de instalación proxy transparente.
- ➢ La solución cubrirá todas las vulnerabilidades expresadas en el OWASP Top Ten más reciente.
- ➢ La solución cumplirá con todos los criterios de evaluación del WAFEC definidos por el *Web Application Security Consortium*.
- ➢ La solución soportará la integración con seguridad para base de datos, del mismo fabricante, para ofrecer seguridad de extremo a extremo; desde internet hasta la base de datos sin ningún cambio en la aplicación web. La seguridad integrada de la base de datos podrá proteger contra ataques conocidos a las bases de datos, deberá también tener capacidad de monitorear y controlar la actividad de la base de datos.
- ➢ La solución proporcionará el bloqueo de direcciones IP, sesiones TCP o usuarios de la aplicación web.
- ➢ La solución protegerá tanto las aplicaciones Web HTTP, como las aplicaciones web SSL y HTTPS.
  - ✓ La solución tendrá la capacidad de recibir y utilizar los certificados y pares de llaves público/privadas para los servidores web protegidos.
  - ✓ La solución podrá descifrar el tráfico SSL, de las aplicaciones web, entre el cliente y el servidor y re-encriptarlo antes de su reenvío.
  - ✓ En los modos puente (bridge) o sniffer, la solución podrá poder descifrar el tráfico SSL para inspección, sin terminar o cambiar la conexión HTTPS.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- ✓ La solución tendrá la capacidad de proteger aplicaciones web que incluyan el contenido de servicios web (xml). La protección XML contará con mecanismos automatizados de aprendizaje, similares a los de la protección de aplicaciones web.
- ✓ La solución soportará la conmutación de datos por error o failover.
- ✓ La solución soportará las opciones fail-open y fail-closed.

➢ La solución contará con funcionalidades que permitan:

- ✓ Rastrear e identificar las fuentes de los ataques originadas desde proxies anónimos, direcciones IP maliciosas, botnets y sitios de phishing.
- ✓ Actualizar las fuentes de ataque para identificar y bloquear el tráfico malicioso.
- ✓ Ajustar dinámicamente las políticas de seguridad con base en la identificación de las fuentes de ataque o de las fuentes que denoten actividad sospechosa.
- ✓ Bloquear solicitudes de acceso basado en la reputación de la fuente del tráfico, como direcciones IP conocidas por su comportamiento malicioso por Botnet, DDoS, Phishing o redes de Anonimización (TOR y Proxies Anónimos).
- ✓ Bloquear solicitudes de acceso basado en el país de origen de la conexión.
- ✓ Realice un análisis automático de distribución de alertas en relación al país de origen, con opción a representar la información a través de un mapa mundial.
- ✓ Detallar y analizar los eventos de seguridad ocurridos, orígenes y método del ataque, dirección IP y localización geográfica del ataque."

➢ La solución podrá:

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- ✓ Inspeccionar y monitorear todos los datos http y la aplicación, incluyendo, los encabezados http, campos de formularios, y el cuerpo http.
- ✓ Inspeccionar las peticiones y respuestas http.
- ✓ Tener la habilidad de decodificar datos a su mínima expresión a partir de diferentes sistemas de encoding Web y validarla.
- ✓ Validar todos los tipos de datos ingresados, incluyento URLs, formularios, cookies, cadenas de queries, campos y parámetros ocultos, métodos http, elementos XML y acciones SOAP.

El **CNS-IPCYT** proporcionará la solución **IMPERVA SecureSphere Hardware Appliance X6510** con el licenciamiento de **Flex Protect Plus for Application and Data Security**, la cual cumple con las características técnicas mencionadas previamente en la presente propuesta.

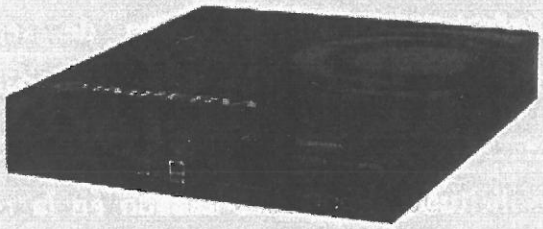


Imagen 5 - Firewall de Aplicaciones Web (WAF)

Referencia: https://www.imperva.com/products/web-application-firewall-waf/

3.6.4. Unidad Integral de firewall de bases de datos.

El **IMSS** requiere de una solución contra las amenazas hacia las bases de datos, que monitoree la actividad local en todos los servidores que: las contengan, alerte y detenga el comportamiento malicioso en tiempo real, además de que funcione en ambientes virtualizados o servicios distribuidos en red, la cual deberá contar con las siguientes características:

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- La solución contará con tecnología de auto-aprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo schemas, objetos, tablas; sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario; todo esto para el establecimiento de un baseline de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.
- La solución incluirá al menos el licenciamiento y soporte que sea compatible con las plataformas de Windows, Linux y Unix.
- Para el caso de crecimiento de la solución de firewall de bases de datos, este deberá estar soportado mediante paquetes de licenciamientos de al menos 10 instancias de bases de datos.
- La solución proporcionará la protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.
- La solución generará reportes y tendencias en tiempo real, así como permitir la modificación de los mismos.
- La solución contará con facilidades o herramientas analíticas para la conducción de análisis forense cuando sea reportado algún incidente.
- La solución podrá no requerir el instalar agentes de software en los servidores a monitorear, pero deberá tener la opción en caso de ser necesario.
- La solución funcionará independiente a la activación de la auditoría nativa de la base de datos.
- La solución será transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
- La solución será capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

comunicación, y configuración de seguridad, sin importar el sistema operativo sobre el que se encuentren instaladas.

- La solución realizará una evaluación exhaustiva de los riesgos de la infraestructura objetivo a diferentes niveles/capas de la infraestructura de base de datos incluyendo:
  - ✓ Cuestiones de configuración de la base de datos tales como nivel de parcheo, configuración de las cuentas de usuario, evaluación de la fortaleza de las contraseñas, vigencia de contraseñas.
  - ✓ Cuestiones de configuración de la plataforma, incluyendo configuración del sistema operativo de los servidores que soportan el software de base de datos.
- La solución podrá realizar descubrimientos automatizados en la red para identificar nuevas bases de datos siendo habilitadas, ya sea a nivel de servidor o puertos habilitados en servidores conocidos.
- La solución tendrá la capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo a las políticas de negocio. Las definiciones de tipo de dato podrán crearse de manera flexible y granular.
- La solución proveerá una solución de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.
- La solución apoyará en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y control de cambios.
- La solución monitoreará toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
- La solución monitoreará e interactuará con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, ligas, stored procedures, entre otros.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- La solución podrá hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.
- La solución tendrá la capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.
- La solución proveerá detalles sobre alertas ya sean falsos positivos o negativos y tendrá la facilidad de cambiar una política desde la alerta.
- La solución manejará reglas y políticas tan amplias o granulares como se requieran y podrán ser construidas automáticamente o manualmente y podrán ser actualizadas, igualmente, de forma manual o automática.
- Las políticas granulares para control de acceso o generación de alertas contarán con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios podrán usarse en cualquier número y cualquier combinación:
  - ✓ Número de registros a regresar por la consulta (SQL Query)
  - ✓ Número de registros afectados
  - ✓ Tipo de datos accesado (financiero, recursos humanos, inventarios, o cualquier definición personalizada)
  - ✓ Acceso a datos marcados como sensibles
  - ✓ Base de Datos, Schema, Instancia, Tabla y Columna accedida
  - ✓ Estado de autenticación de la sesión
  - ✓ Usuario y/o Grupo de Usuarios de Base de Datos conectado
  - ✓ Usuario conectado en la capa aplicativa, a diferencia del usuario conectado a la DB
  - ✓ Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier personalización por expresiones regulares)
  - ✓ Logins, Logouts, Queries
  - ✓ IPs de origen y destino
  - ✓ Nombre de Host origen, Usuario firmado en el Host origen

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- ✓ Aplicación usada para la conexión a la base de datos
- ✓ Tiempo de respuesta/procesamiento del query
- ✓ Errores en el manejador de SQL
- ✓ Número de ocurrencias en intervalos de tiempo definidos
- ✓ Por operaciones básicas (Select, Insert, Update, Delete)
- ✓ Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export)
- ✓ Por Stored Procedure o Function utilizada
- ✓ Si existe ticket asignado de cambios
- ✓ Hora del Día

- ➢ La solución identificará individualmente a los usuarios finales que realicen actividades mediante aplicaciones, aún si utilizan mecanismos comunes de comunicación entre la aplicación y la base de datos, esta actividad no implicará la modificación de la aplicación y/o de la base de datos.
- ➢ La solución podrá posibilitar los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.
- ➢ La solución podrá asociar y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son indicativos de una potencial violación de seguridad.
- ➢ La solución protegerá contra ataques SQL y no-SQL (como buffer overflow).
- ➢ La solución correlacionará la actividad en base de datos con actividad de aplicaciones web para entender detalladamente como los usuarios están accediendo datos privilegiados sin necesidad de alterar la aplicación web.
- ➢ Considerados de emergencia para potenciales violaciones de la información que incluyan, enunciativa mas no limitativamente:
  - ✓ Altos volúmenes de acceso a datos sensibles más allá de lo habitual.
  - ✓ Acceso a datos inusual para cierta hora del día.
  - ✓ Acceso a datos desde una ubicación (física) desconocida.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- ✓ Acceso a datos utilizando aplicaciones/herramientas no autorizadas.

- La solución manejará una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.
- La solución podrá tener facilidades de Archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP).
- La solución contará con Políticas, Reportes, Alertas, Objetos Sensibles, y Transacciones pre-identificadas y pre-configuradas para trabajar con las siguientes plataformas empresariales: Oracle EBS, Peoplesoft, SAP, SQL, entre otras.
- La solución tendrá la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.
- La solución analizará los eventos generados desde diferentes bases de datos. El análisis contemplará los siguientes criterios:
  - ✓ Mostrar el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos.
  - ✓ Contar con un sistema de correlación basado en la dirección de los ataques. Deberá determinar si los ataques provienen desde dentro de la organización hacia afuera de la misma o viceversa.
  - ✓ Realizar una correlación automática y en tiempo real de eventos, vulnerabilidades y bases de datos.
  - ✓ Ejecutar una correlación que permita identificar usuarios de aplicación asociados con consultas –y determinadas actividades– en bases de datos específicas sin necesidad de alterar aplicaciones o instalar API's.
  - ✓ Correlacionar eventos como número de errores inusuales de sentencias de SQL o al momento de hacer login a las bases de datos.
- La solución permitirá el manejo de alarmas y notificaciones –en tiempo real– para los eventos de correlación mencionados anteriormente.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- La solución tendrá la capacidad de monitorear aplicaciones web en la misma solución, ofreciendo una visibilidad, seguridad y control desde el usuario web hasta la base de datos.
- La solución contará con un módulo de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de las mismas.
- La solución soportará y aplicará simultáneamente un modelo de seguridad positivo y negativo.
- El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que deberá además cumplir con las siguientes especificaciones:
  - ✓ Bloquear las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
  - ✓ Incluir una lista pre-configurada y detallada de las firmas de ataque.
  - ✓ Permitir la modificación o adición de firmas por el administrador.
  - ✓ Permitir la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
  - ✓ Detectar ataques conocidos en múltiples niveles, incluyendo, la red, sistemas operativos, software del servidor web y ataques a nivel de aplicación.
- La solución soportará Gateway clúster a nivel de los agentes de monitoreo de Bases de Datos, es decir que los agentes estarán asignados a un Gateway y podrán moverse automáticamente o manualmente según sea el caso sin necesidad de volver a registrar el agente con el Gateway o realizar alguna acción en el servidor en el cual se encuentra instalado el agente.
- La solución proporcionará un proceso de instalación, actualización y gestión de cambios centralizada, segura y ágil para los Agentes; la cual proporcionará una visión completa de todas las actualizaciones disponibles para los componentes de la solución de protección de Bases de Datos.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- La solución notificará cuando se encuentre disponible una nueva versión de Agente.
- El despliegue y la instalación centralizada de parches y actualizaciones a componentes solo será realizada por usuarios con los privilegios necesarios y administradores de la herramienta.
- La solución proporcionará información del tráfico enviado de los Agentes a los Gateways, identificando actividades de Bases de Datos que no son necesarias monitorear; permitiendo a los administradores de la solución generar reglas de exclusión para reducir el consumo de recursos en el servidor.
- La solución contará con la opción de reducir el tráfico entre la comunicación entre el Agente y el Gateway utilizando métodos de comprensión de datos.
- La solución proporcionará la opción de enmascarar la información personal que se despliega atreves de la interfaz de administración, además deberá contar con la opción de desenmascarar esta información dependiendo los privilegios de cada usuario.

La solución propuesta por el **CNS-IPCYT**, la cual cumple con los requerimientos descritos en los puntos anteriores es el firewall de bases de datos (DBF) de la marca **IMPERVA SecureSphere Hardware Appliance X6510** con el licenciamiento de **Flex Protect Plus for Application and Data Security.**

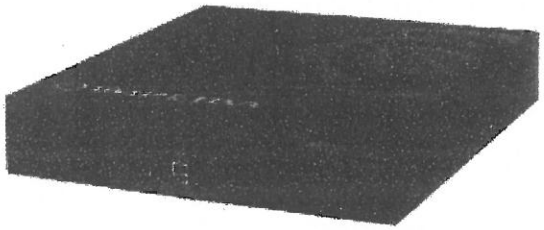


Imagen 6 - Firewall de Bases de Datos (DBF)

Referencia: https://www.imperva.com/docs/DS_Database_Security_ES.pdf

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.7. UNIDAD INTEGRAL DE BALANCEO DE CARGAS EN COMUNICACIONES.

El **IMSS** requiere la solución de Balanceo de carga L4-L7 para aplicaciones Web o equivalente y su información inherente. La infraestructura propuesta deberá cumplir con las siguientes especificaciones técnicas mínimas:

- La solución de balanceo de carga propuesta estará en alta disponibilidad.
- El equipamiento propuesto será de propósito específico; es decir que la tecnología propuesta será dedicada en funcionalidad para el balanceo de carga de capas 4 a capa 7 del modelo OSI, por lo que no se aprovisionara dispositivos con tecnologías cortafuegos (firewalls), sistemas de prevención y detección contra intrusos (IPS) y las variantes o combinaciones como firewall de gestión unificada de amenazas (Unified Threat Management o UTM, por sus siglas en inglés), firewalls de próxima generación (Next Generation Firewall o NGFW, por sus siglas en inglés), sistemas de prevención de próxima generación (Next Generation IPS o NGIPS por sus siglas en inglés), firewall de aplicación (Web Application Firewall o WAF, por sus siglas en inglés).
- La tecnología propuesta cumplirá con la arquitectura diseñada y desarrollada por el fabricante con el único y exclusivo propósito de balanceo de cargas.
- Adicionalmente, la solución soportará la funcionalidad de alta disponibilidad para obtener un mejor nivel de disponibilidad.
- El equipamiento soportará al menos 650,000 de peticiones (capa 7 del modelo OSI) por segundo.
- El equipamiento soportará al menos 250,000 conexiones por segundo.
- El equipamiento tendrá un desempeño de 10 Gbps.
- El equipamiento propuesto contará con fuente de poder redundante
- El **CNS-IPCYT** deberá aprovisionar toda la infraestructura necesaria la cual deberá ser nueva y cumplir al 100% con las características mínimas necesarias descritas en el presente documento para ofrecer la solución de balanceador de cargas.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.8. UNIDAD DE COMPONENTE INTEGRAL DE PUNTO NEUTRO

El **IMSS** requiere establecer comunicación desde diferentes ubicaciones o localidades remotas hacia el centro de datos ofertado, donde podrán converger distintos carrier's. En este punto de la red, tendrá que proporcionar a través de su infraestructura de red LAN el transporte de datos, video y voz que se reciban de los distintos **CNS-IPCYTS** de enlaces de comunicación.

Esta red, será responsable de alojar la acometida del servicio de Internet con la que hoy cuenta el **IMSS**, 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 propuestas en cuanto a capacidad, funcionalidad, operación y disponibilidad de la solución propuesta serán las siguientes:

Incluirá interfaces físicas redundantes, con infraestructura de comunicaciones en alta disponibilidad dedicada, con capacidad instalada para operar al menos lo siguiente:

- 48 interface RJ45 en cobre a velocidad de al menos 1 Gbps,
- 48 interface Ópticas a velocidad 1 o 10 Gbps.
- 6 clases de Servicio MPLS.
- Infraestructura "Nonblocking".
- Interconexión de componentes en Malla con enlaces de alta capacidad 40 y 100 Gbps.
- Capacidad de conectar al menos 35 Redes MPLS.
- Capacidad de conectar al menos 35 Enlaces Punto a Punto. (ruteables).
- Capacidad de conectar al menos 35 Enlaces L2L.
- Capacidad para recibir 1000 usuarios de VPN "site to site" en IPSEC de diferentes fabricantes de equipo.
- Capacidad de recibir 1000 usuarios de VPN "cliente to site" en IPSEC con dispositivos móviles.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- 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.
- 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.

Tendrá la capacidad y disponibilidad de interactuar en conjunto con otro **CNS-IPCYT** de servicios para lograr automatizar la redundancia a las comunicaciones tanto en la capa de WAN como la de Internet.

Las políticas de acceso serán las estipuladas por el Centro de Datos del **CNS-IPCYT** donde será alojada la infraestructura del **IMSS**.

El equipamiento soportará recibir al menos los siguientes servicios:

1 enlace redundante a Internet con un ancho de banda inicial de 1 Gbps y un máximo de 10 Gbps.

- Deberá recibirse con Interfaces físicas necesarias en cobre (RJ45) u ópticas (MTRJ) compatibles con la velocidad al menos de 1 Gbps y de 10 Gbps.
- En caso de requerirse uno o más tendidos nuevos o reubicaciones de cableado ya sea UTP o fibra óptica, deberá proporcionarse con cables categoría 6 y multinodo respectivamente, las Interfaces en cobre (RJ45) u ópticas (MTRJ) que soporten al menos la velocidad al menos de 1 Gbps y de 10 Gbps.
- La Infraestructura de equipo de comunicaciones deberá proporcionarse en alta disponibilidad.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

2 enlaces LAN to LAN redundantes con un ancho de banda inicial de 1 Gbps y un máximo de 10 Gbps.

- Deberá recibirse con Interfaces físicas necesarias en cobre (RJ45) u ópticas (MTRJ) compatibles con la velocidad al menos de 1 Gbps y de 10 Gbps.
- En caso de requerirse en Punto Neutro uno o más tendidos nuevos o reubicaciones de cableado ya sea UTP o fibra óptica, deberá proporcionarse con cables categoría 6 y multinodo respectivamente, las Interfaces en cobre (RJ45) u ópticas (MTRJ) que soporten al menos la velocidad al menos de 1 Gbps y de 10 Gbps.
- La Infraestructura de equipo de comunicaciones deberá proporcionarse en alta disponibilidad.

2 enlaces MPLS redundantes con un ancho de banda inicial de 500 Mbps y un máximo de 10 Gbps.

- Deberá recibirse con Interfaces físicas necesarias en cobre (RJ45) u ópticas (MTRJ) compatibles con la velocidad al menos de 1 Gbps y de 10 Gbps.
- En caso de requerirse en Punto Neutro uno o más tendidos nuevos o reubicaciones de cableado ya sea UTP o fibra óptica, deberá proporcionarse con cables categoría 6 y multinodo 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.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- En caso de requerirse uno o más tendidos nuevos o reubicaciones de cableado ya sea UTP o fibra óptica, deberá proporcionarse con cables categoría 6 y multinodo 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 centro de datos del **CNS-IPCYT** cuenta con las características solicitadas en los puntos anteriores y cuenta con la capacidad de crecimiento modular en caso de ser necesario.

3.9. UNIDAD DE ENLACES DEDICADOS CON UNA CAPACIDAD DE 5 GBPS

El **CNS-IPCYT** aprovisionara la infraestructura necesaria para habilitar la solucion de Enlace LAN to LAN (L2L), la cual permitirá la una extensión del direccionamiento LAN del sitio del **IMSS** que se trate. Lo anterior con el fin de mantener el mismo dominio de "broadcast" mediante un enlace Ethernet. Las interfaces proporcionadas podran ser ópticas o en Ethernet.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

Las características que se incluirán son al menos son las siguientes:

- Interfaces físicas 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.
- Direccionamiento IP privado con la validación del **IMSS.**
- Capacidad de conectar al menos 1 (un) enlace "LAN to LAN" con una capacidad de 5 Gbps.
- Monitoreo de red y análisis de tráfico.
- Acceso al centro de datos con doble trayectoria.
- Niveles de disponibilidad mensual de 99.90%.
- Infraestructura dedicada.
- El apego a las políticas de acceso físicas serán las estipuladas por el **CNS-IPCYT** en acuerdo con el **IMSS**.
- La solución podrá recibir en una capa extra de seguridad por medio de un clúster de firewalls que permita realizar DMZ independientes por enlace con el fin de acotar mediante políticas de "firewall" los accesos por puertos TCP/IP a las aplicaciones de la contratante.
- El **CNS-IPCYT** 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.
- La definición de los puntos de interconexión será revisada en conjunto entre el **CNS-IPCYT** y el **IMSS**.

El servicio incluirá la infraestructura de hardware y software necesaria para poder proporcionar todas las funcionalidades arriba descritas y además deberá incluir la

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

instalación, implementación, puesta a punto, administración, mantenimiento y soporte para el servicio y la infraestructura involucrada para su prestación.

3.10. UNIDAD DE SOPORTE

El soporte deberá contar con las siguientes características mínimas:

- El **CNS-IPCYT** deberá recibir solicitudes de servicio por parte del **IMSS** vía telefónica y correo electrónico, mediante un punto único de contacto (Centro de soporte del **CNS-IPCYT**). El tiempo de respuesta para el seguimiento de solicitudes deberá ser inmediato, el **CNS-IPCYT** deberá contar con una matriz de escalamiento. El centro de soporte del **CNS-IPCYT** ganador deberá contar con disponibilidad ininterrumpida para la recepción de solicitudes de soporte en horario de 7x24.
- El **IMSS** podrá realizar solicitudes de soporte para obtener asistencia telefónica, o por correo electrónico por parte del **CNS-IPCYT**, provisto a través de personal certificado.
- En caso de que el soporte técnico requerido esté relacionado con fallas de hardware, el **CNS-IPCYT** deberá remplazar sin costo alguno para el **IMSS** el equipo dañado por uno de iguales o mejores características, para cubrir los niveles de servicio solicitados.
- En caso de falla de hardware/software el **CNS-IPCYT** deberá estar disponible en un horario de 7x24 para el remplazo de las partes dañadas con un tiempo de solución no mayor a 4 horas una vez que el **IMSS** haya reportado la falla al centro de atención del **CNS-IPCYT**, el **CNS-IPCYT** tendrá un tiempo no mayor a 15 minutos para el registro del ticket correspondiente, así como su seguimiento con la mesa de servicio del **IMSS**.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

Características mínimas del centro de soporte del CNS-IPCYT.

El **CNS-IPCYT** debe contar con un Centro de Atención permanente durante las 24 horas del día y durante la vigencia del contrato, debiendo proporcionar el soporte técnico que corresponda al horario y vigencia de la contratación del servicio, a través del cual el **IMSS** pueda levantar reportes para solicitar soporte en sitio en caso de falla y Asesoría Técnica Telefónica (ilimitada e inmediata).

El **CNS-IPCYT** debe brindar un tiempo de respuesta inmediato sin catalogar por grado de severidad la contingencia presentada, comprometiéndose a presentarse en sitio en un tiempo máximo de 4 horas cuando así lo solicite el **IMSS**; asimismo el **IMSS** podrá solicitar al **CNS-IPCYT** que el servicio se realice en el horario que más le convenga.

En caso de que el **CNS-IPCYT** del servicio no pueda resolver el problema y se requiera el apoyo directo del fabricante, el **IMSS** deberá tener acceso por medio del **CNS-IPCYT** adjudicado a los servicios de soporte y atención del fabricante, así como acceso a su centro de atención.

a) **Solicitudes de servicio**

Entiéndase como solicitud de servicio, de forma enunciativa más no limitativa, toda aquella que el **IMSS** solicite a la mesa de ayuda del **CNS-IPCYT** y que no sea motivo de incidente activo.

Dentro de estas solicitudes de servicio están las siguientes:

- Solicitud de desempeño de la infraestructura propuesta que componen los diferentes servicios descritos en la presente propuesta.
- Solicitud de revisión de LOGS de las diferentes soluciones propuestas.
- Solicitud de reportes de incidentes y/o problemas de todos los servicios descritos en el presente documento.
- Altas, Bajas y Cambios en la infraestructura que compone los servicios descritos en la presente propuesta.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Y cualquier solicitud relacionada con cada servicio que compone el proyecto.

Estas solicitudes deben ser atendidas en tiempo y forma con base en lo acordado en el **IMSS** y el **CNS-IPCYT**.

3.11. TRANSFERENCIA DE CONOCIMIENTO Y ADIESTRAMIENTO TÉCNICO

El **CNS-IPCYT** establecerá un plan para la transferencia de conocimiento y adiestramiento técnico en las diferentes herramientas, tecnologías de la información y/o componentes con las cuales se bridará el servicio, impartiendo y transfiriendo el conocimiento al personal técnico definido por el **IMSS**, todo esto para al menos 15 personas por tema, y entregando en su propuesta el listado de temas, nombre, número o identificador de curso por tecnología propuesta, así como la duración en horas de cada uno de estos.

La transferencia de conocimiento y adiestramiento técnico, será, preferentemente en español o en su caso, en idioma inglés, con un enfoque a los componentes de la plataforma virtualizada que integran el servicio.

Con el objetivo de no frenar el avance del proyecto, la etapa de transferencia de conocimiento se establecerá con el **CNS-IPCYT** de forma posterior a la implementación y estabilización de los servicios, coordinando y estableciendo fechas y sedes.

Los cursos podrán ser teóricos y/o teórico-prácticos y podrán ser impartidos en las instalaciones del **IMSS** en la Ciudad de México o de acordarse con el **IMSS** de forma remota, según sea más conveniente.

El **CNS-IPCYT** proporcionará los contenidos o materiales informativos de la transferencia de conocimientos a abordar a cada uno de los participantes, ya sea que el expositor sea personal directo del fabricante o bien, una persona certificada.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.12. TRANSFERENCIA DE CONOCIMIENTO TECNOLÓGICO EN PLATAFORMAS DE CÓDIGO ABIERTO (VIRTUALIZACIÓN, CONTENEDORES, SERVIDORES WEB, SERVIDORES DE APLICACIÓN, SISTEMAS OPERATIVOS, BASES DE DATOS, ETC., EJEMPLO: RED HAT O EQUIVALENTE)

El **CNS-IPCYT** incluirá los temarios para la ejecución de la transferencia de conocimiento, los cuales serán analizados, modificados o en su caso aceptados por parte del Instituto en las mesas de trabajo al inicio del contrato. Los temas a considerar deberán estar relacionados con la virtualización, contenedores, servidores web y de aplicación, sistemas operativos, bases de datos u otros que pudiesen existir dentro de la solución propuesta o sujetos a consideración del Instituto.

3.13. TRANSFERENCIA DE CONOCIMIENTO EN SEGURIDAD

El **CNS-IPCYT** implementará y proporcionar la integración de temas que puedan estar relacionados a los servicios que se enlistan a continuación:

- Servicio de Firewalls de siguiente generación
- Servicio de protección contra ataques DDoS
- Servicio de redes virtuales privadas
- Servicio de Antispam
- Servicio de filtrado WEB
- Servicio de Firewall de aplicaciones web
- Servicio de Firewall de bases de datos
- Servicio de balanceador de carga de capas L4 – L7

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.14. REPOSITORIOS

3.14.1. REPOSITORIO DOCUMENTAL

El **CNS-IPCYT** proporcionará mediante el establecimiento de una plataforma (repositorio) los documentos probatorios del servicio, como lo pueden ser entregables, informes, reportes, entre otros, o en su caso, el Instituto definirá el repositorio correspondiente. La plataforma que servirá de contenedor oficial será administrada y soportada por el **CNS-IPCYT.**

La plataforma (repositorio) contará con accesos controlados y definidos por el Instituto, para asegurar la confidencialidad de los documentos que ahí se resguarden, manejando bitácoras de actividad, accesos a documentos, entre otras estadísticas, debiendo entregar cuando menos 3 copias en medio electrónico, al Instituto al término del contrato, independientemente de la entrega que deberá realizar al proveedor que vaya a dar continuidad a este servicio al término del contrato.

3.14.2. REPOSITORIO DE IMÁGENES DE CONTENEDORES

El **CNS-IPCYT** proporcionará el espacio en una plataforma de acceso compartido, donde se resguardará el software utilizado durante la operación del proyecto. La plataforma que servirá de contenedor será administrada, operada y soportada por el **CNS-IPCYT** siendo asignado espacio de la infraestructura asignada para los servicios.

La plataforma (repositorio) contará con accesos controlados y definidos por el Instituto, para asegurar la confidencialidad de la información que ahí se resguarden, manejando bitácoras de actividad, accesos a documentos, entre otras estadísticas.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

3.14.3.BASE DE CONOCIMIENTOS TÉCNICOS DE RESPUESTA RÁPIDA PARA PUBLICACIÓN DE SOLUCIONES RÁPIDAS (CONSTRUCCIÓN DE UNA BASE DE CONOCIMIENTOS)

El **CNS-IPCYT** realizará las actividades técnicas necesarias para gestionar el conocimiento operativo relacionado a la ejecución de los procesos de soporte, operación y pruebas de la migración; así como con los sistemas informáticos que los sustentan; para que dicho conocimiento sea creado, capturado, transformado y utilizado para brindar visibilidad sobre la operación y los resultados de las pruebas de migración y buscar e identificar áreas de oportunidad para mejorar y sustentar la toma de decisiones respecto a su modelos operativo, etapa de pruebas y migración.

El **CNS-IPCYT** planificará, proveerá e implantará, las herramientas tecnológicas necesarias para sustentar el ciclo de vida de dicho conocimiento; así como definir y diseñar los modelos ontológicos y taxonómicos para representar y clasificar el conocimiento tomando en consideración de los modelos establecidos por el propio **IMSS**. Para tales propósitos, se deberán incluir por lo menos los siguientes activos:

- Iniciativas
- Información del contrato o contratos relacionados y acuerdos de trabajo
- Productos y artefactos
- Minutas y evidencias de trabajo y colaboración
- Reportes de incidentes
- Reportes de problemas
- Tableros de indicadores de operación
- Base de datos de gestión de configuraciones (CMDB)

La información anterior es de manera enunciativa más no limitativa y podrán incluirse tópicos según se defina en las mesas de planeación de arranque del contrato.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

Estos servicios soportan el modelo de control del contrato del servicio, a través de la integración y revisión de los reportes y demás documentos que formalizan los entregables que soporten el pago de los servicios que valide el Administrador del Contrato.

3.14.4. *CMBD DE INFRAESTRUCTURA TECNOLÓGICA.*

El **CNS-IPCYT** realizará las acciones necesarias para el diseño, planeación, habilitación, configuración, implementación, operación, gestión, soporte y actualización de la CMBD, en infraestructura habilitada por el **CNS-IPCYT** y accesible tanto a personal del **CNS-IPCYT** como del INSTITUTO de las Coordinación de Sistemas de Infraestructura Tecnológica Institucional (CSITI) y/o de la Coordinación de Ingeniería Tecnológica (CIT).

El **CNS-IPCYT** ejecutará las actividades y un plan para la carga inicial y periódica de los Elementos de Configuración (CIs) de la infraestructura tecnológica física y virtual relacionada al servicio.

El **CNS-IPCYT** entregará de manera mensual un reporte que muestre las altas, bajas o modificación de los elementos de configuración (CIs) durante el periodo.

El **CNS-IPCYT** expondrá a través de la Intranet del **IMSS**, la CMDB a manera de blog para consulta únicamente al personal que el Instituto designe.

3.15. SOPORTE, OPERACIÓN Y MONITOREO DE SERVICIOS DIGITALES, ASÍ COMO SUS COMPONENTES LÓGICOS SOBRE LAS PATAFORMAS DE CÓDIGO ABIERTO

El **CNS-IPCYT** contemplará los requerimientos necesarios para brindar el soporte a los componentes principales de las capas de aplicaciones.

El **CNS-IPCYT** contemplará la segregación de las aplicaciones en base a su complejidad, área de negocio, criticidad y afectación en el periodo estacional, haciendo un criterio de asignación de soporte en base a niveles de experiencia de usuarios, siendo dividas en:

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- 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 contiene múltiples elementos a migrar dentro de sus capas tecnológicas.
- Mediano; Aplicaciones que dentro de su proceso de migración involucran la migración de datos y que son consideradas aplicaciones críticas dentro del IMSS. 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 IMSS.

El IMSS dentro de lo solicitado como soporte comprende las siguientes categorías con sus diversas aplicaciones actuales susceptibles a las pruebas de migración y en su caso las aplicaciones que sean actualizadas acorde al marco tecnológico de referencia del Instituto, mismo que se definirá en las mesas de arranque del contrato, los siguientes elementos se muestran de manera enunciativa más no limitativa son:

- Gestión de recursos
  - Gestión de identidades
    a. Open AM
    b. Oracle IDM
    c. NetIQ Access Manager Appliance (Access Gateway)
  - Gestión de Infraestructura
    a. Red Hat Cloudforms
    b. Nodos Ansible
- Análisis, reporteo y estadísticas
  - Reportes a la medida (Ad-hoc)

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

a. Microsoft Reporting Services
b. ESSBase
c. Hyperion

- Inteligencia de negocio
  - Visualización y Análisis de Información
  - Oracle Business Intelligence
  - Microsoft Analisys Services
  - SAS
  - Oracle Exalytics In-Memory Machine
  - Soporte a la toma de decisiones
- Soporte a la toma de decisiones
  - Tableau Server
  - Tableau Desktop
- Análisis estadístico
  - Stata
- Gestión de datos
  - Extracción, transformación y carga de datos (ETL)

a. Oracle ODI
b. IBM Data Stage
c. Microsoft Integration Services
d. Oracle Warehouse Builder
e. Integración y Transformación de Información
f. Redbrick
g. Stata Transfer

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Integración e intercambio de datos
  a. Oracle Golden Gate
- Gestión de la calidad de los datos
  a. Oracle Data Quality
- Sistema de gestión de bases de datos
  a. Bases de Datos Oracle
  b. Microsoft SQL Serve
  c. DB2
  d. Subscripciones a Bases de Datos Open Source
  e. Oracle Exadata Storage Expansion
  f. SQL Server Parallel Data Warehouse
- Directorio
  a. Open DJ
  b. NetIQ Access Manager (Identity Provider)
  c. Plataforma LDAP
  d. Herramientas y entorno de desarrollo
  e. Entorno de desarrollo integrado (IDE)
  f. Team Foundation Server
- Kit de Desarrollo de Software (SDK)
  a. Java Development Kit
  b. Java Enterprise Edition
  c. Java.Runtime Environment
  d. .NET Framework
- Gestión de documentos y contenidos
  a. Gestión de contenidos Web

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- ✓ Drupal
- ✓ Liferay Enterprise
- ✓ Adobe ColdFusion

- Middleware
  a. Bus de servicios empresariales (ESB)
     - ✓ Oracle Service Bus
     - ✓ Oracle ALSB
     - ✓ Oracle ALDS
     - ✓ Red Hat JBOSS Fuse
     - ✓ SOA Suite
- Software de mensajería
  a. Apache Kafka
- Interfaz o descripción de servicios
  a. Oracle Enterprise Repository
  b. Oracle Service Registry
  c. Red Hat JBoss SOA Enterprise
- Servidores de Aplicaciones
  a. WebLogic
  b. Tuxedo
  c. GlassFish
  d. Red Hat JBOSS Enterprise Application
  e. Apache Tomcat
  f. Apache HTTPD
  g. Oracle Exalogic
- Automatización y gestión de procesos

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

a. Gestión de procesos de negocios (BPMS)
   - ✓ Oracle BPM
   - ✓ Red Hat JBOSS BPM Suite

- Gestión de reglas de negocio
  a. Motor de Reglas
- Comunicación unificada y colaboración
  a. Correo electrónico
     - ✓ Servicio de correo electrónico

Para brindar y garantizar el soporte a las aplicaciones, el **CNS-IPCYT** contemplará perfiles técnicos calificados, certificados y con grados de experiencia acorde a las complejidades de los ambientes, componentes, servicios y aplicativos del Instituto.

3.16. DISEÑO Y PRUEBAS DE UN PLAN DE RECUPERACIÓN DE DESASTRES Y UN PLAN DE CONTINUIDAD DEL NEGOCIO PARA EL IMSS.

El **CNS-IPCYT** esté situado en un lugar con bajo riesgo o vulnerabilidad ante fenómenos de origen geológico o naturales como pueden ser: sismos, tsunamis o maremotos, vulcanismos, entre otros.

- El **CNS-IPCYT** desarrollará e implementar la metodología para lograr una recuperación de las operaciones y funciones esenciales o críticas del Instituto, en caso de desastres o contingencias.
- El **CNS-IPCYT** elaborará y entregar un plan de trabajo para la generación del "Plan de Recuperación ante Desastres o Contingencias" (DRP), considerando entre otros:
  - Criterios de notificación y escalación para la declaración de un desastre o contingencia y activar los procesos de recuperación,

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- La definición de las estrategias de respaldo y de recuperación de sistemas e infraestructura esencial o crítica, física y/o lógica de recuperación de los sistemas centralizados y descentralizados
- El plan de retorno y, pruebas del plan y su respectivo mantenimiento y actualización.
- El DRP será documentado con base en un mínimo de 5, a un máximo de 10 escenarios de desastre.

- El **CNS-IPCYT** realizará una prueba de escritorio y posterior a ésta, realizará una prueba en vivo, siempre y cuando El **CNS-IPCYT** y el Instituto cuenten con los elementos necesarios y haya sido establecida la planificación de la prueba; se deberán elegir el o los escenarios de desastre o de la contingencia, las estrategias de respaldo y de recuperación, y llevar a cabo la documentación de los resultados de ésta y de los hallazgos identificados durante su ejecución. El alcance de la prueba será definido previo a su ejecución, considerando como mínimo un proceso esencial o crítico y como máximo el total de los procesos críticos definidos por el Instituto.
- Para el desarrollo del "Plan de Recuperación ante Desastres o Contingencias" (DRP), El **CNS-IPCYT**, incluirá la identificación de los activos de información necesarios y ubicados en los centros de datos del Instituto y en instalaciones de sus proveedores de centro de datos, que permitan soportar la solución de recuperación definida, con la adecuada coordinación de los equipos encargados de la continuidad operativa y que no estén bajo responsabilidad del **CNS-IPCYT**, además El **CNS-IPCYT** será responsable de dar soporte durante las pruebas, asignando los recursos humanos idóneos en cantidad y competencias profesionales.
- El **CNS-IPCYT** elaborará y entregará el documento de nombre "Plan de Continuidad de Negocio" (BCP); este plan incluirá la documentación necesaria para trabajar de forma manual, de forma electrónica y en papel, la definición de procedimientos alternos, flujos de comunicación identificando los roles y responsabilidades del personal crítico, los recursos físicos y tecnológicos mínimos necesarios, así como la verificación de sitios alternos internos y/o externos.
- El **CNS-IPCYT** incluirá en su metodología a implementar las siguientes actividades: Análisis de Riesgos, Análisis de Impacto al Negocio, Planeación de la Continuidad de Negocio y de recuperación, considerando, además las estrategias de respaldo y de recuperación de sistemas e infraestructura, física y virtualizada, de los sistemas

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

centralizados y descentralizados y por último las pruebas de los planes y su respectivo mantenimiento.

- Recomendar diferentes alternativas tecnológicas para instrumentar la capacidad de recuperación en caso de desastre, conforme a la definición y metodología propuesta por el **CNS-IPCYT** y aprobada por el **IMSS** para el Desarrollo del Plan de Recuperación de Desastres (DRP) y del Plan de Continuidad del Negocio (BCP) del **IMSS**.

3.17. ESPECIFICACIONES TÉCNICAS

COMPONENTE O SERVICIO	DESCRIPCIÓN	ESPECIFICACIÓN	TIPO
Servicios de operación	Establecen las especificaciones, calendarios, niveles de servicio, arquitecturas y lineamientos técnicos para la contratación de los servicios necesarios para la operación de la infraestructura lógica	Gestión de servicios de Tecnologías de la Información	Funcional

3.18. ESPECIFICACIONES TÉCNICAS PARA TODAS LAS SOLUCIONES

El **CNS-IPCYT** deberá ejecutar las acciones que permitan tener la calidad necesaria en el suministro instalación y configuración de todas las soluciones requeridas y garantizar la confidencialidad, integridad y disponibilidad de los servicios que se describen la presente propuesta, con la finalidad de brindar continuidad operativa a los servicios utilizados por el **IMSS**, privilegiando los tiempos, especificaciones y prioridades establecidas por el **IMSS**.

El **CNS-IPCYT** deberá monitorear el estado de los equipos que integran todos los servicios de tal manera que se generen acciones proactivas para corregir fallas sobre los servicios ofertados. Por lo que el **CNS-IPCYT** deberá considerar todos los componentes y aditamentos necesarios para su diseño, implementación y puesta en marcha.

El **CNS-IPCYT** deberá incluir personal certificado por cada tecnología propuesta a implementarse con el objeto de garantizar que, desde la planeación, diseño,

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

implementación y puesta en marcha se cumplan con todos los requerimientos descritos en la presente propuesta.

El **CNS-IPCYT** deberá incluir todas las adecuaciones eléctricas necesarias para la incorporación de los equipos que forman parte del servicio de aprovisionamiento, tales como conectores hembra/macho y así como las adecuaciones a los PDU´s de interconexión eléctrica) existentes en el centro de datos del **CNS-IPCYT**.

El **CNS-IPCYT** deberá de considerar todas las actualizaciones (updates y demás elementos en software sobre el mismo release o en release diferente) que realice el fabricante con respecto de los bienes objeto del presente documento y en su caso deberá de llevarlos a cabo al momento de su estabilidad en caso de ser compatible con la infraestructura adquirida por el período de contratación antes señalado.

El **CNS-IPCYT** deberá incluir todo el licenciamiento relacionado al equipamiento propuesto de hardware, software y comunicaciones, requeridos para el cumplimiento de funcionalidades y su adecuada operación de **todos los componentes que integran la solución** por un periodo de al menos la vigencia del contrato.

El **CNS-IPCYT** deberá incluir al recurso humano necesario para la implementación de los servicios de aprovisionamiento, el cual deberá contar con la experiencia necesaria para la implementación del equipamiento propuesto.

4. PLAN DE ASEGURAMIENTO DE LA CALIDAD

4.1. CONDICIONES GENERALES

El **CNS-IPCYT** proveerá de los insumos y equipos necesarios para el aprovisionamiento del equipamiento propuesto. Los incidentes y solicitudes se gestionarán para su atención a través de una mesa de servicios o centro de operaciones del **CNS-IPCYT**. Todo el soporte técnico preventivo, correctivo, así como partes, refacciones y consumibles serán incluidos.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

El **CNS-IPCYT** ejecutará las acciones que permitan tener la calidad necesaria y garantizar la confidencialidad, integridad y disponibilidad requerida de los servicios que se describen en la presente propuesta.

El CNS-IPCYT de servicios podrá monitorear el estado de los equipos de tal manera que se generen acciones proactivas para corregir fallas sobre la red de área local, seguridad, de la cual se proporcionará la arquitectura actual.

El CNS-IPCYT cuenta con amplia experiencia en la implementación y puesta a punto de servicios especificados en la presente propuesta, así como contar con la ingeniería certificada en las tecnologías ofertadas.

El CNS-IPCYT incluirá un administrador de proyectos certificado en Project Manager Professional (PMP) por el Project Management Institute (PMI). Así mismo, presentará su certificación vigente durante la vigencia del contrato.

El CNS-IPCYT es dueño de un centro de datos certificado por el UPTIME INSTITUTE con el nivel de TIER III, el cual se utilizará para hospedar el equipamiento especificado en el aprovisionamiento del equipamiento propuesto en la presente propuesta.

Por lo que **el CNS-IPCYT** considerará todos los componentes y aditamentos necesarios para su administración, configuración y operación.

4.1.1. CUMPLIMIENTO DE OBLIGACIONES CONTRACTUALES

Para la documentación de Cumplimiento de Obligaciones contractuales, que permita una fácil y organizada atención de procesos de auditoria por parte de los entes de fiscalización, el **CNS-IPCYT** elaborará en un plazo no mayor a 15 (quince) días hábiles posteriores a la adjudicación del contrato, una matriz de los verbos, pronombres, tiempos y compromisos presentes en el anexo técnico, términos y condiciones, apéndices o documentación complementaria al anexo, a fin de contar con un listado de todos los verbos de acción,

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

conjunciones, excepciones, interacciones, consideraciones de tipo y frecuencia de información electrónica que deba incluirse, casos de uso y en su caso especificaciones o excepciones, para convertirlos en los "documentos probatorios de cada obligación establecida en el contrato".

A partir de este listado, de manera conjunta entre el **IMSS** y el **CNS-IPCYT**, en un plazo no mayor a 10 (diez) días hábiles 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 **CNS-IPCYT** 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 **CNS-IPCYT**, 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 **CNS-IPCYT** 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 **CNS-IPCYT**, habilitará al menos 3 pantallas de al menos 75 pulgadas, con todo lo necesario para la presentación de información de la operación de los servicios tecnológicos que permitan exponer de manera gráfica y ágil lo descrito en los dos párrafos anteriores, lo que permitirá contar con información en línea constante de la operación de los servicios contratados incluyendo elementos de análisis y detalles de la operación (parámetros de utilización) de la

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

infraestructura ofertada además de la prestación de los servicios, preferentemente reflejando la operación en términos de infraestructura física o virtual (según corresponda) además de indicadores de negocio que puedan ser descritos desde el alcance de cada contrato.

4.1.2. CLÁUSULAS Y CUMPLIMIENTOS

a. **Contrato de confidencialidad**

El **CNS-IPCYT** en conjunto con el **IMSS** firmarán un Contrato de confidencialidad mediante el cual el **CNS-IPCYT** se obliga a no revelar, transferir, compartir ni ceder ningún dato o información de carácter sensible y confidencial que se hayan compartido entre el **CNS-IPCYT** y el **IMSS**.

b. **Cláusula de Opción para Obtención de Bienes al cierre de contrato (entregable de infraestructura)**

Una vez concluida la prestación del servicio, el **CNS-IPCYT** realizará un proceso de entrega de todo el equipamiento que haya sido incorporado como parte del proyecto. Llámese cualquier componente de hardware/software que integre dicho servicio descrito en el presente documento, así como en la propuesta del proveedor. El **CNS-IPCYT** deberá sujetarse al procedimiento que el **IMSS** requiera para formalizar este proceso.

c. **Documentación de cumplimiento de obligaciones**

El **CNS-IPCYT** con el objeto de fortalecer la supervisión y vigilancia de la administración del contrato materia del presente servicio y contribuir a las acciones para verificar la procedencia de los pagos, proporcionará un soporte especializado para la gestión del conocimiento administrativo relacionado con la prestación de los servicios de Nube **IMSS**.

Para que dicho conocimiento administrativo sea traducido en un activo del **IMSS**, el **CNS-IPCYT** aplicará el modelo de control de contratos definido por la Coordinación de Sistemas de Infraestructura Tecnológica Institucional (o la correspondiente por funciones

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

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 **CNS-IPCYT** 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 **CNS-IPCYT** 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 **CNS-IPCYT** 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 **CNS-IPCYT** no cuenta con la documentación probatoria de los servicios devengados, estos no podrán ser facturados.
- **Plataforma de obligaciones:** En este apartado, el **CNS-IPCYT** elaborará un listado que identifique la totalidad de las obligaciones que se encuentran plasmadas en el

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

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 coincidan el pago de los servicios, sin embargo, su cumplimiento es obligatorio en términos del instrumento contractual.

El **CNS-IPCYT** presentará la documentación descrita en el presente punto, previo a solicitar el pago de sus servicios.

Asimismo, el **CNS-IPCYT** 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 **CNS-IPCYT** 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 **CNS-IPCYT** 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

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

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 **CNS-IPCYT** 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 **CNS-IPCYT** 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 **CNS-IPCYT** 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

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

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 **CNS-IPCYT** 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.

4.2. ACEPTACIÓN

La aceptación de la solución propuesta se dará cuando el **IMSS** valide por cada plataforma tecnológica lo siguiente:

- Se dará por aceptado la solución cuando todos los componentes 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 la presente propuesta y se realice entrega de las memorias técnicas correspondientes, 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 la solución será supervisada por personal que el **IMSS** asigne.

4.3. LICENCIAMIENTO

La solución ofertada por el **CNS-IPCYT** considerará la totalidad de licencias de la solución integral para brindar todos los requerimientos establecidos en la presente propuesta. La vigencia del licenciamiento para todos los servicios deberá ser al menos el tiempo de la

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

vigencia del contrato. En caso de que el diseño final validado por personal del **IMSS** requiera de licenciamiento adicional para el correcto funcionamiento de todos sus componentes será proporcionado por el **CNS-IPCYT** sin un costo adicional al **IMSS**.

4.4. PROCESOS

El CNS-IPCYT entregará toda la documentación que se genere por parte del durante la vigencia del contrato y estará apegada a los formatos y procesos de **MAAGTIC-SI**. Los formatos que solicita el **IMSS** referentes al **MAAGTIC-SI** son los que actualmente están vigentes, sin embargo, al momento de la contratación y durante la vigencia del contrato dichos formatos solicitados en la presente propuesta podrán actualizarse, cancelarse, modificarse, sustituirse y/o en su caso incrementarse los formatos de acuerdo a los lineamientos que establezca la **Secretaría de la Función Pública**.

La documentación generada por el aprovisionamiento del equipamiento deberá apegarse a los procesos vigentes del **MAAGTIC-SI**, los cuales se describen a continuación:

- Solicitud de Incidentes
- Administración de la Configuración
- Control de Cambios
- Administración de la Seguridad de la Información
- Operación de Controles de Seguridad de la Información y ERISC

4.5. RECURSOS HUMANOS

El CNS-IPCYT incluirá los Recursos Humanos necesarios para la implantación, puesta en marcha del servicio de Servicio de Infraestructura Física para la migración de la Nube **IMSS** y DRP 2020 de acuerdo a los tiempos y niveles de servicio establecidos. El personal que realice funciones de coordinación, supervisión o cualquier otra función similar o superior que **el CNS-IPCYT** proporcione, deberá tener el enfoque de atención a clientes, servicio y amplio conocimiento técnico y operativo.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

Este personal será sujeto a entrevista y aprobación de parte del **IMSS**; el cual solo formará parte del equipo de trabajo una vez que se realice el visto bueno por el **IMSS**.

En caso de existir algún inconveniente con el personal este deberá ser reemplazado en caso de que el área lo solicite. Este cambio deberá realizarse en un plazo no mayor a 10 días hábiles.

El CNS-IPCYT contará con personal calificado en las tecnologías del equipamiento propuesto para atender los incidentes presentados en la infraestructura, para lo cual deberá atender y resolver dichos incidentes las veces que sea necesario. Las certificaciones que cuenta el **CNS-IPCYT** son las siguientes de forma enunciativas más no limitativas:

- CCIE Seguridad
- CCIE Routing and Switching
- CCIE Service Provider
- CCNP Colaboración
- CCDP Diseño Profesional de redes.
- CCNA Cyber Ops
- ITIL Foundation Certificate in IT Service Management
- Symantec Data Loss Prevention 14.5
- Symantec Messaging Gateway
- APDS - Avaya Networking Solutions
- APSS - Avaya Networking Solutions
- ISO/IEC 27001
- ISO/IEC 20000
- ITIL intermediate in-Service Design
- ITIL intermediate in Operational support and analysis
- ITIL intermediate in Service Offering AND Agreements
- ITIL intermediate un Release, control and validation.
- PCNSE Network Security Engineer 7
- MCITP Enterprise Administrator on Windows Server 2008
- MCTS Microsoft Exchange Server 2007 Configuration
- Extreme Networks Design Specialist - Campus Fabric
- Enterasys Certified Specialist – Routing
- Enterasys Certified Specialist – Policy.
- Security Competency – Technical Accreditation (SCT)
- Network Automation Competency – Technical Accreditation (NCT)
- Core Network Services Competency - Technical Accreditation (CNT)
- Certificación ITIL RCV, 2017

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

- Certificación ITIL SO, 2016
- Certificación ITIL SOA, 2016
- Certificación ITIL OSA, 2012
- Project Management Professional del PMI

Es importante señalar que con base en las necesidades de las unidades responsables de del **IMSS** esta lista podrá ser modificada de tal manera que puede solicitarse la rotación de personal o el movimiento temporal de los técnicos especialistas para atender eventos que así lo requieran.

El CNS-IPCYT deberá considerar que el **IMSS** podrá requerir el apoyo de los ingenieros fuera de los días y horario mencionado para la atención del *Servicio* (Por eventos especiales, reubicaciones, servicios temporales, etc), por lo que este tipo de solicitudes deberán estar consideradas por **el CNS-IPCYT**. Para ello el **IMSS** notificará con un periodo de 24 horas de anticipación.

El CNS-IPCYT proporcionará el personal que atienda incidentes durante las 24 horas (7x24x365). por lo que deberán estar disponibles y en caso de presentarse un incidente fuera del horario establecido como principal, se presentarán en un periodo no mayor a dos horas después a de la notificación.

4.6. CRONOGRAMA DE ACTIVIDADES

Las actividades para la ejecución están categorizadas en 9 grandes etapas que se mencionan a continuación.

1. Entrega y recepción de documentación posterior a la adjudicación
2. Mesas de trabajo del inicio del contrato
3. Acuerdos de Niveles de Servicio con otros proveedores del Instituto
4. Establecimiento de matrices de escalación, procedimientos de atención en la mesa de servicio, establecimiento de grupos de soporte.
5. Establecimientos de órdenes de trabajo iniciales

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

6. Calendario, plan de trabajo, establecimiento de compromisos tales como: instalación, configuración y puesta a punto de la plataforma de virtualización
7. Plan de trabajo para las labores de BCP y DRP
8. Pruebas de BCP y DRP sobre la plataforma de virtualización
9. Mesas de trabajo para el cierre del contrato.

5. NIVELES DE SERVICIO

El proceso de Administración del Nivel del Servicio deberá involucrar tanto al **CNS-IPCYT** como al **IMSS** para mantener y monitorear el adecuado funcionamiento del servicio. El **CNS-IPCYT** mantendrá una revisión continúa de los logros de servicio para garantizar que la calidad del servicio sea mantenida y mejorada permanentemente.

5.1. NIVEL GENERAL DE SERVICIO

Los niveles de servicio establecidos que deberá cumplir el **CNS-IPCYT** en la prestación de los servicios es el siguiente:

El nivel de servicio base para este contrato es de:

NIVEL DE DISPONIBILIDAD	MINUTOS INDISPONIBLES PERMITIDOS EN EL MES PARA LOS SERVICIOS DEL PRESENTE CONTRATO
99.982% sobre la plataforma instalada (TIER III)	7.8 minutos

Esta disponibilidad establecida incluye el servicio de soporte técnico en caso de falla en un esquema de 5x8 en días y horarios hábiles con soporte presencial certificado, por lo que en su caso, será exigible la participación de especialistas únicamente en estos horarios, sin embargo, puede requerirse presencia en un esquema 7x24 del personal asociado al servicio, a petición del Instituto.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

Los niveles de servicio para la atención tickets, incidentes, atención de requerimientos se detalla a continuación.

CRITICIDAD	Tipo de Cobertura	Cobertura	Tiempo de registro del evento (minutos naturales)	Tiempo de diagnóstico (horas naturales)	Tiempo de solución o sustitución a partir del diagnóstico (horas naturales)
TIPO DE CRITICIDAD DEL SERVICIO		Horarios de atención para los incidentes	Tiempo de registro del evento (llamada telefónica / correo electrónico)	Tiempo de diagnóstico del incidente a partir de levantamiento del reporte (considera colocar equipo de respaldo temporal)	Tiempo en el que debe de solucionar o sustituir un equipo, configuración o infraestructura lógica por diagnóstico de falla irreparable o fuera de soporte
ALTA	**7x24xVigencia del contrato**	0:00 a 24:00	10	2	2
MEDIA	**5x8 xVigencia del Contrato**	0:00 a 24:00	10	3	4
BAJA	**5x8 xVigencia del Contrato**	0:00 a 24:00	10	4	8

El **CNS-IPCYT** cumplirá con los tiempos de respuesta solicitados por el **IMSS.**

Por "TIEMPOR DE REGISTRO DEL EVENTO" se entenderá como el tiempo máximo transcurrido desde el momento en que el **IMSS** o las herramientas de monitoreo automatizadas reportan una falla o desviación en el desempeño de los ambientes virtualizados lógicos (el que ocurra primero), se registre el evento en su herramienta de mesa de servicio y notifique al **IMSS** el número de ticket para su atención, de acuerdo al

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

procedimiento para el reporte de fallas o de herramientas automatizadas para el monitoreo.

Por "TIEMPO DE DIAGNOSTICO" se entenderá el tiempo máximo transcurrido desde el momento en que el **CNS-IPCYT** notifique al **IMSS** el número de ticket para su atención y hasta el momento en que personal del **CNS-IPCYT** efectúe el diagnóstico o determinación del plan de solución y lo haga de conocimiento del **IMSS**.

Por "TIEMPO DE SOLUCIÓN' se entenderá el tiempo máximo transcurrido desde el momento en que el **CNS-IPCYT** efectúe el diagnóstico o determinación del plan de solución, y hasta el momento en que personal del **CNS-IPCYT** ya sea de manera remota o en SITIO, haya finalizado las acciones necesarias para dejar el SERVICIO operando de acuerdo a su funcionalidad normal. En caso de ser necesario, el **CNS-IPCYT** podrá sustituir alguna infraestructura física o virtual de manera total o parcial por otro de igual o superiores características, y podrá realizar las adecuaciones necesarias a la configuración para conseguir su funcionalidad normal de operación.

El **CNS-IPCYT** contará con una base de conocimientos, la cual se deberá actualizar de forma dinámica con el propósito de reducir tiempos de respuesta en los incidentes.

6. DEDUCTIVAS POR INCUMPLIMIENTO DE NIVELES DE SERVICIOS

La siguiente tabla clasifica las deductivas aplicables de manera particular a los servicios del presente documento.

ACCIONES	NIVEL DE SERVICIO	DEDUCTIVA
Validación de Componentes de Infraestructura física (**)	- A más tardar 24 horas naturales posteriores a la notificación.	- El equivalente a 10% del costo del servicio por deficiencias en la validación de componentes de infraestructura física.
Instalación de Infraestructura Virtual (**)	- A más tardar 24 horas naturales posteriores a la solicitud del servicio, de conformidad al marco (stack) tecnológico definido.	- El equivalente a 10% del costo del servicio por desviaciones de la infraestructura entregada Vs el marco (stack) tecnológico definido.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

Configuración y Puesta a Punto de Infraestructura Virtual (**)	- A más tardar 24 horas naturales posteriores a la solicitud de configuración y puesta a punto.	- El equivalente a 10% del costo del servicio por desviaciones de la configuración y puesta a punto de la infraestructura virtual.
Tunning de Infraestructura Virtual (**)	- A más tardar 24 horas naturales posteriores a la solicitud de tunning de infraestructura virtual o en su caso el periodo que se defina de común acuerdo entre el **CNS-IPCYT** y autorizado por el Instituto.	- El equivalente a 10% del costo del servicio por desviaciones de tunning de infraestructura virtual.
Actualización y Mantenimiento de Infraestructura Virtual (**)	- A más tardar 24 horas naturales posteriores a la detección de desviaciones en el desempeño operativo de la infraestructura virtual o en su caso el periodo que se defina de común acuerdo entre el **CNS-IPCYT** y autorizado por el Instituto.	- El equivalente a 10% del costo del servicio por desviaciones de actualización o mantenimiento de infraestructura virtual, cuya afectación o impacto sea menor. - El equivalente a 30% del costo del servicio por desviaciones de actualización o mantenimiento de infraestructura virtual, cuya afectación o impacto sea Medio. - El equivalente a 50% del costo del servicio por desviaciones de actualización o mantenimiento de infraestructura virtual, cuya afectación o impacto sea Mayor. Lo anterior, de acuerdo a la matriz de impacto establecida en las mesas de planeación.
Gestión de Incidentes de la Infraestructura Virtual (Lógica)	- De acuerdo a la severidad de afectación y a las matrices de escalación y de impacto definida en las mesas de planeación del arranque. - Nivel de servicio 99.9 de disponibilidad en horario hábil (5x8).	- El equivalente a 2.5% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio. - El equivalente a 10% del costo del servicio por desviaciones en la gestión de incidentes de la infraestructura virtual, cuya afectación o impacto sea menor. - El equivalente a 30% del costo del servicio por desviaciones en la gestión de incidentes de la infraestructura virtual, cuya afectación o impacto sea Medio. - El equivalente a 50% del costo del servicio por desviaciones en la gestión de incidentes de la infraestructura virtual, cuya afectación o impacto sea Mayor. Lo anterior, de acuerdo a la matriz de impacto establecida en las mesas de planeación.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

Configuración de Redes y Telecomunicaciones Virtuales	- De acuerdo a la complejidad o en su caso a los tiempos establecidos por el Instituto y el proveedor acorde al impacto definido en las mesas de planeación del arranque.	- El equivalente a 10% del costo del servicio por desviaciones en la Configuración de Redes y Telecomunicaciones Virtuales, cuya afectación o impacto sea menor. - El equivalente a 30% del costo del servicio por desviaciones en la Configuración de Redes y Telecomunicaciones Virtuales, cuya afectación o impacto sea Medio. - El equivalente a 50% del costo del servicio por desviaciones en la Configuración de Redes y Telecomunicaciones Virtuales, cuya afectación o impacto sea Mayor. Lo anterior, de acuerdo a la matriz de impacto establecida en las mesas de planeación.
Aprovisionamiento de Infraestructura Virtual	- A más tardar 24 horas naturales posteriores a la solicitud del servicio, de conformidad al marco (stack) tecnológico definido.	- El equivalente a 10% del costo del servicio por desviaciones de la infraestructura entregada Vs el marco (stack) tecnológico definido.
Servicio de Respaldo y Restauración	- Configuración de políticas, a más tardar 06 horas naturales posteriores a la solicitud del servicio. - Ejecución de respaldos, iniciar a más tardar 3 horas naturales posteriores a la hora indicada en el respaldo para su ejecución, en la política de respaldo asociada. - Ejercicio de restauración, iniciar a más tardar 12 horas posteriores a la solicitud del ejercicio por parte del Instituto. - Restauraciones bajo demanda, iniciar a más tardar 01 hora posterior a la solicitud del Instituto. - La operación del servicio deberá ser 24x7x365, con un nivel de servicio al menos de 99.9%	- El equivalente a 10% del costo del servicio por desviaciones en la restauración de la información Vs el requerimiento realizado por el Instituto (Política de respaldo), cuyo afectación o impacto sea bajo. - El equivalente a 30% del costo del servicio por desviaciones en la restauración de la información Vs el requerimiento realizado por el Instituto (Política de respaldo), cuyo afectación o impacto sea medio. - El equivalente a 50% del costo del servicio por desviaciones en la restauración de la información Vs el requerimiento realizado por el Instituto (Política de respaldo), cuya afectación o impacto sea mayor. Lo anterior, de acuerdo a la matriz de impacto establecida en las mesas de planeación.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

Estación de Trabajo Equipada	- A más tardar 02 horas posteriores a la solicitud del servicio.	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido.
Monitoreo y Reporteo de Infraestructura Virtual	- A más tardar 05 días naturales posteriores a la solicitud del servicio. - El detalle y la periodicidad de los reportes serán definidos en las mesas de trabajo al inicio del contrato. - La operación del servicio deberá ser 24x7x365, con un nivel de servicio al menos de 99.9%	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido. Siempre y cuando no haya habido un requerimiento de ventana de mantenimiento debidamente autorizado por el Instituto.
Habilitación y operación de centros de monitoreo en instalaciones del IMSS en Reforma 476 ó en las instalaciones que determine el Instituto.	- A más tardar 30 días naturales posteriores a la solicitud del servicio. - La operación del servicio deberá ser 24x7x365, con un nivel de servicio al menos de 99.9%	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido. Siempre y cuando no haya habido un requerimiento de ventana de mantenimiento debidamente autorizado por el Instituto.
Tablero de Consumo Tendencias de Infraestructura Virtual y Gasto	- Para su inicio: A más tardar 20 días naturales posteriores a la solicitud del servicio. - Para su actualización: A más tardar 10 días naturales posteriores a la solicitud del servicio. - La operación del servicio deberá ser 24x7x365, con un nivel de servicio al menos de 99.9%	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido. Siempre y cuando no haya habido un requerimiento de ventana de mantenimiento debidamente autorizado por el Instituto.
Sizing y Arquitectura de Infraestructura Virtual	- La operación del servicio deberá ser 5x8, con un nivel de servicio al menos de 99.9% - Deberá informar que los parámetros de operación exceden los rangos establecidos en las mesas de trabajo al inicio del contrato. - Deberá ejecutar el cambio de arquitectura o redimensionamiento (resizing)	- El equivalente a 10% del costo del servicio mensual cuando no informe que los parámetros de operación exceden los rangos establecidos en las mesas de trabajo al inicio del contrato. - El equivalente a 30% del costo del servicio mensual cuando no se ejecute el cambio de arquitectura o redimensionamiento (resizing) previa autorización del Instituto. - El equivalente a 20% del costo del servicio mensual cuando se ejecute el

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

	previa autorización del Instituto.	redimensionamiento o el cambio de arquitectura y se presenten afectaciones de baja criticidad. - El equivalente a 30% del costo del servicio mensual cuando se ejecute el redimensionamiento o el cambio de arquitectura y se presenten afectaciones de mediana criticidad. - El equivalente a 50% del costo del servicio mensual cuando se ejecute el redimensionamiento o el cambio de arquitectura y se presenten afectaciones de alta criticidad. El nivel de afectación se determinará de conformidad a las matrices de impacto que se definan en las mesas de trabajo al inicio del contrato.
Administrador de Proyectos	- Reporte diario de avance de proyectos (el detalle se definirá en las mesas de planeación del arranque). - Reunión semanal de seguimiento de proyectos que incluya además de lo anterior presupuesto, recursos y tiempo.	- El equivalente a 10% del costo mensual del servicio por deficiencias en la veracidad del reporte y la información.
Representante de Servicios en Sitio	- Informe diario de avance de proyectos que incluya presupuesto, recursos, tiempo, incidentes, cambios, problemas y desviaciones (el detalle se definirá en las mesas de planeación del arranque). - Reunión semanal de seguimiento de proyectos.	- El equivalente a 10% del costo mensual del servicio por deficiencias en la veracidad del informe.
Documentación de Cumplimiento de Obligaciones	- La documentación del cumplimiento de obligaciones, el detalle se definirá en las mesas de planeación del arranque. - Elaboración y firma de los Acuerdos Operacionales (OLAs) durante las mesas de planeación (a más tardar a 03 semanas posteriores a la notificación del	- Por deficiencias en la veracidad de cada documento que acredite el cumplimiento de obligaciones (entregables), se aplicará una deductiva equivalente a 5% del costo mensual del servicio de infraestructura virtual.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

	fallo). - Elaboración de reporte de cumplimiento de los acuerdos operacionales (por proveedor). - Elaboración mensual del cumplimiento de obligaciones.	
Repositorio Documental	- El inicio de operaciones del Repositorio Documental será en la fecha establecida en las mesas de planeación del arranque. -La actualización periódica del Repositorio Documental deberá realizarse de acuerdo a lo establecido en las reuniones de gobierno del contrato, las cuales se efectuarán semanalmente. - La operación del repositorio documental deberá ser 5x8, con un nivel de servicio al menos de 99.9%	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido. - Por deficiencias en la veracidad de la documentación contenida en el repositorio, se aplicará una deductiva equivalente a 10% del costo mensual del servicio.
Servicio de Entrega al Cierre de Contrato	- La documentación del cumplimiento de obligaciones, el detalle se definirá en las mesas de planeación del arranque. -Listado de compromisos contractuales y el estado que guardan al cierre del contrato, cumplimiento de entregables.	- Por deficiencias en la veracidad de cada documento que acredite el cumplimiento de obligaciones (entregables), se aplicará una deductiva equivalente a 5% del costo mensual del servicio de infraestructura virtual.
Transferencia de Conocimiento y Adiestramiento Tecnológico	- Las fechas de entrenamiento se definirán en las mesas de planeación del arranque.	- Por deficiencias en la impartición del entrenamiento tecnológico se aplicará una deductiva del 30% del costo del servicio, la deficiencia se determinará mediante la aplicación de encuestas de satisfacción a los participantes del curso, en caso que el promedio de la evaluación sea menor a 80%.
Contrato de Confidencialidad	- Cumplimiento de la confidencialidad por parte de ambas instituciones durante la vigencia establecida en el convenio de confidencialidad.	- En caso del incumplimiento de la confidencialidad establecida, se aplicará una deductiva equivalente al 10% del valor máximo del contrato.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

Soporte empresarial de la solución de virtualización que incluya transferencia de conocimiento.	- La contratación del soporte empresarial deberá ser a más tardar en la fecha establecida en las mesas de trabajo de inicio del contrato. - La operación del soporte deberá ser el establecido entre el **IMSS** y el **CNS-IPCYT** Adjudicado en las mesas de trabajo de inicio del contrato. - Las fechas de entrenamiento se definirán en las mesas de planeación del arranque.	- El equivalente a 10% del costo mensual del servicio de soporte fuera del nivel de servicio establecido entre el **IMSS** y el **CNS-IPCYT** Adjudicado en las mesas de trabajo de inicio del contrato. - Por deficiencias en la impartición del entrenamiento tecnológico se aplicará una deductiva del 30% del costo del servicio, la deficiencia se determinará mediante la aplicación de encuestas de satisfacción a los participantes del curso, en caso que el promedio de la evaluación sea menor a 80%.
CMDB de Infraestructura Lógica	- La entrega de la CMDB inicial se deberá realizar en el plazo acordado en las mesas de trabajo al inicio del contrato. - La actualización periódica de los elementos de configuración (CMDB) deberá realizarse de acuerdo a lo establecido en las reuniones de gobierno del contrato, las cuales se efectuarán semanalmente.	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido.
Base de FAQs para Publicación de Soluciones Rápidas	- La entrega de la Base de FAQs para Publicación de Soluciones Rápidas inicial se deberá realizar en el plazo acordado en las mesas de trabajo al inicio del contrato. - La actualización periódica de los elementos de la Base de FAQs para Publicación de Soluciones Rápidas deberá realizarse de acuerdo a lo establecido en las reuniones de gobierno del contrato, las cuales se efectuarán semanalmente.	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

Repositorio de Imágenes de Contenedores	- La entrega de la Base de FAQs para Publicación de Soluciones Rápidas inicial se deberá realizar en el plazo acordado en las mesas de trabajo al inicio del contrato. - La actualización periódica de los elementos de la Base de FAQs para Publicación de Soluciones Rápidas deberá realizarse de acuerdo a lo establecido en las reuniones de gobierno del contrato, las cuales se efectuarán semanalmente.	- El equivalente a 10% del costo mensual del servicio por punto porcentual o fracción fuera del nivel de servicio establecido.

(**) El marco de referencia para estas definiciones, serán perfeccionados o particularizados en las mesas de trabajo realizadas al inicio del respectivo contrato, sin embargo, de manera general, tendrán el siguiente alcance:

Validación de Componentes de Infraestructura física: Se refiere a la actividad de comprobar que la infraestructura física entregada por parte del **CNS-IPCYT** adjudicado correspondiente a la infraestructura física, cumple con las características solicitadas por el **IMSS** y se encuentra listo para ser configurado de manera lógica o virtual.

Instalación de Infraestructura Virtual: Se refiere a la actividad de virtualización de la infraestructura física entregada por parte del **CNS-IPCYT** adjudicado correspondiente a la infraestructura física, de tal manera que, pueda entregar servicios lógicos o virtuales utilizables por el **IMSS**, en general, son instalaciones por default o con parámetros de fábrica, que si bien permiten un uso por parte del **IMSS**, podrían ser optimizados en el contexto del ecosistema tecnológico Institucional.

Configuración y Puesta a Punto de Infraestructura Virtual: Se refiere a la actividad(es) de realizadas por parte del **CNS-IPCYT** para que la infraestructura virtualizada pueda ser usada para los fines definidos por el **IMSS**, optimizando las instalaciones por default o con parámetros de fábrica, que si bien permiten un uso por parte del **IMSS**, podrían se.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

optimizados en el contexto del ecosistema tecnológico Institucional, a fin de garantizar la continuidad operativa de esta infraestructura virtual dentro del ecosistema operativo.

Operación de Infraestructura Virtual: Se refiere a la actividad de mantener la continuidad operativa de la infraestructura virtualizada dentro de los parámetros de operación y desempeño establecidos para este fin.

Tunning de Infraestructura Virtual: Se refiere al ajuste y optimización periódico (al menos cada tres meses o cada que se detecte un incidente de desviación de los niveles de desempeño establecidos en el presente documento, incluyendo el correcto dimensionamiento de la infraestructura física o virtual) de la infraestructura virtualizada (hipervisor, contenedor, sistemas operativos huésped, software especializado, sistemas, aplicativos, servicios, bases de datos, web services, servidores de aplicación, balanceadores, es decir, todo aquello que se encuentre contenido en la infraestructura física entregada para su virtualización) en operación y que permita tener un mejor desempeño de los ambientes virtualizados de conformidad a los parámetros definidos en el ecosistema tecnológico Institucional.

Actualización y Mantenimiento de Infraestructura Virtual: Se refiere a las actividades de mantener la infraestructura virtualizada (actualizaciones, parches, configuraciones, parámetros, dimensionamiento y todo lo relacionado a la correcta operación del sistema o de los servicios virtualizados) en las últimas versiones liberadas y estables por parte del fabricante del hipervisor, contenedor, sistemas operativos huésped, software especializado, sistemas, aplicativos, servicios, bases de datos, web services, servidores de aplicación, balanceadores, es decir, todo aquello que se encuentre contenido en la infraestructura física entregada para su virtualización.

Gestión de Incidentes de la Infraestructura Virtual (Lógica): Se refiere a todas a las actividades relacionadas al seguimiento y solución de los eventos, incidentes y problemas que se presenten en la infraestructura virtualizada o en uno de sus componentes o hipervisor, contenedor, sistemas operativos huésped, software especializado, sistemas,

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

aplicativos, servicios, bases de datos, web services, servidores de aplicación, balanceadores, es decir, todo aquello que se encuentre contenido en la infraestructura física entregada para su virtualización.

Configuración de Redes y Telecomunicaciones Virtuales: Se refiere a la actividad(es) de realizadas por parte del **CNS-IPCYT** para que la infraestructura virtualizada de Redes y Telecomunicaciones pueda ser usada para los fines definidos por el **IMSS**, optimizando las instalaciones por default o con parámetros de fábrica, que si bien permiten un uso por parte del **IMSS**, podrían ser optimizados en el contexto del ecosistema tecnológico Institucional, a fin de garantizar la continuidad operativa de esta infraestructura virtual dentro del ecosistema operativo.

7. REQUERIMIENTOS DE ARQUITECTURA TECNOLÓGICA

N/A

8. RESTRICCIONES E INTERFACES CON OTROS ELEMENTOS

N/A

9. PROCESO DE ENTREGA AL TÉRMINO DEL CONTRATO

Una vez concluida la prestación del servicio, el **CNS-IPCYT**, entre otras cosas, realizará un proceso de entrega de todo el equipamiento, software, configuración, desarrollos, CMDB, base de datos de conocimiento, diagramas, bases de conocimiento de configuración de: hipervisor, contenedor, sistemas operativos huésped, software especializado, sistemas, aplicativos, servicios, bases de datos, web services, servidores de aplicación, balanceadores, monitoreo y en general de todas las herramientas y funcionalidades de todo lo que haya sido incorporado como parte del proyecto o en su caso, producto del servicio, incluyendo cualquier componente de hardware/software que integre dicho servicio descrito en el presente documento, así como en la propuesta del proveedor. El **CNS-IPCYT** deberá sujetarse al procedimiento que el **IMSS** requiera para formalizar este proceso.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

10. DOCUMENTOS DE SOPORTE Y ENTREGABLES

10.1. ENTREGABLES Y MODELO DE GOBIERNO DEL CONTRATO

Los documentos que deberá presentar el **CNS-IPCYT** de servicio, son reportes que permitan identificar el monitoreo de la infraestructura, por lo que se hace indispensable la entrega mensual de cada uno de los siguientes reportes listados a continuación:

ENTREGABLE	FECHA DE ENTREGA	MEDIO
Transferencia de conocimiento	Como máximo 2 semanas después de la implementación. (Única Ocasión)	Electrónico e impreso
Memorias Técnicas de la configuración e instalación de la plataforma de virtualización.	Como máximo 10 días posteriores al mes en curso.	Electrónico e impreso

Estos entregables cumplirán con los lineamientos y procesos que indica el **MAAGTIC-SI.**

10.2. REQUISITOS PARA LOS ENTREGABLES

El **CNS-IPCYT** deberá cubrir con las siguientes consideraciones para el concepto de entregables:

- Entregará 1 CD o DVD y 1 copia, debidamente etiquetada, conteniendo los entregables del mes.
- Entregará un resumen ejecutivo impreso dentro de una carpeta el cual acompañará al CD o DVD.
- El formato y contenido de los archivos electrónicos mensuales deberán contener al menos las secciones descritas a continuación:
- Información del documento
- Servicio: Deberá indicarse el servicio del cual se trata el documento.
- Clave y nombre del documento: Los documentos podrán referenciarse con una clave y nombre.

Camino a la Presa San José 2055, Col. Lomas 4a sección, CP. 78216, San Luis Potosí S.L.P., Tel.: (444) 834 20 00,
www.ipicyt.edu.mx

SIN TEXTO

GOBIERNO DE MÉXICO | IMSS

DIRECCIÓN DE ADMINISTRACIÓN
UNIDAD DE ADQUISICIONES E INFRAESTRUCTURA
COORDINACIÓN DE INVESTIGACIÓN DE MERCADOS
COORDINACIÓN TÉCNICA DE INVESTIGACIÓN DE MERCADOS
DIVISIÓN DE INVESTIGACIÓN DE MERCADOS DE ADQUISICIONES Y ARRENDAMIENTOS

Sección I "Precios Unitarios"
Instituto Mexicano del Seguro Social - Dirección de Innovación y Desarrollo Tecnológico (DIDT)

Id	Concepto	Cantidad Mínima	Cantidad Máxima	Precio Unitario de Referencia ($ M.N.)	Tipo de Precio	Unidad	Costo Mínimo Ofertado	Costo Máximo Ofertado	Precio Unitario para Cálculo en Base al Costo del Servicio	Costo Mínimo con Descuento de Precio Ofertado	Costo Máximo con Descuento de Precio Ofertado
S1	Red Hat Ansible Automation Standard (100 Managed Nodes)	100	300	$260,000.00	Unitario	Suscripción	$260,000.00	$780,000.00	$10.00	$260,010.00	$780,010.00
S2	Red Hat Virtualization Suite with Guest and Management (2 sockets), Standard	12.00	24.00	$111,040.00	Unitario	Suscripción	$1,332,480.00	$2,664,960.00	$10.00	$1,332,600.00	$2,665,200.00
S3	Red Hat OpenShift Container Platform with Integration, Standard (64 cores or 128 vCPUs)	2.00	4.00	$3,801,600.00	Unitario	Suscripción	$7,603,200.00	$15,206,400.00	$10.00	$7,603,220.00	$15,206,420.00
S4	Red Hat OpenShift Container Storage Standard (2 Core)	2.00	24.00	$36,000.00	Unitario	Suscripción	$72,000.00	$864,000.00	$10.00	$72,020.00	$864,240.00
S5	Servicio de Instalación de RHOS	12.00	24.00	$60,000.00	Unitario	Suscripción	$720,000.00	$1,440,000.00	$0.00	$720,000.00	$1,440,000.00
S6	Servicio de Instalación de RHOP	4.00	8.00	$160,000.00	Unitario	Suscripción	$640,000.00	$1,280,000.00	$0.00	$640,000.00	$1,280,000.00
S7	Enlace de 1 GB	2.00	4.00	$610,000.00	Unitario	Servicio de Instalación	$1,220,000.00	$2,440,000.00	$0.00	$1,220,000.00	$2,440,000.00
S8	Servicio de Configuración de Redes Virtuales	1.00	2.00	$1,500,000.00	Unitario	Paquete de Horas de Ingeniería	$1,500,000.00	$3,000,000.00	$0.00	$1,500,000.00	$3,000,000.00
S9	Punto Neutro	1.00	2.00	$4,000,000.00	Unitario	Servicio de Instalación	$4,000,000.00	$8,000,000.00	$0.00	$4,000,000.00	$8,000,000.00
S10	Servicio de Soporte a Software	2.00	4.00	$2,650,000.00	Unitario	Paquete de Horas de Ingeniería	$5,300,000.00	$10,600,000.00	$0.00	$5,300,000.00	$10,600,000.00
S11	Servicio de Asesoría Técnica Especializada en Sitio	2.00	4.00	$196,000.00	Unitario	Paquete de Horas de Ingeniería	$392,000.00	$784,000.00	$0.00	$392,000.00	$784,000.00
						Subtotal	$23,036,680.00	$46,087,360.00		$23,036,880.00	$46,087,680.00
						IVA	$3,685,868.80	$7,373,977.60		$3,685,900.80	$7,374,028.80
						Total	$26,722,548.80	$53,461,337.60		$26,722,780.80	$53,461,708.80

ANEXOS
DIVISION DE CONTRATOS
ANEXOS
DIVISION DE CONTRATOS

GOBIERNO DE MÉXICO | IMSS

DIRECCIÓN DE ADMINISTRACIÓN
UNIDAD DE ADQUISICIONES E INFRAESTRUCTURA
COORDINACIÓN DE INVESTIGACIÓN DE MERCADOS
COORDINACIÓN TÉCNICA DE INVESTIGACION DE MERCADOS
DIVISIÓN DE INVESTIGACIÓN DE MERCADOS DE ADQUISICIONES Y ARRENDAMIENTOS

CRITERIO DE ESTRATIFICACIÓN				
Tamaño	Sector	Rango de número de trabajadores	Rango de monto de ventas anuales (Cifras en millones de pesos)	Tope máximo combinado*
Micro	Todas	Hasta 10	Hasta 4	4.6
Pequeña	Comercio	11 hasta 30	Desde 4.01 hasta 100	93
	Industria y Servicios	Desde 11 hasta 50	Desde 4.01 hasta 100	95
Mediana	Comercio	Desde 31 hasta 100	100.01 Hasta 250	235
	Servicios	Desde 51 hasta 100	100.01 Hasta 250	235
	Industria	Desde 51 hasta 250	100.01 Hasta 250	250

*Tope Máximo Combinado = (Trabajadores) X 10% + (Ventas Anuales) X 90%).
El número de trabajadores será el que resulte de la sumatoria de los puntos.
El Tamaño de la empresa se determinará a partir del puntaje obtenido conforme a la siguiente fórmula:
Puntaje de la empresa = (Número de trabajadores) X 10% + (Monto de Ventas Anuales) X 90% el cual debe ser igual o menor al Tope Máximo Combinado de su categoría.

Criterios de Estratificación

GOBIERNO DE MÉXICO | IMSS

DIRECCIÓN DE ADMINISTRACIÓN
UNIDAD DE ADQUISICIONES E INFRAESTRUCTURA
COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS
COORDINACIÓN TÉCNICA DE ADQUISICIÓN DE BIENES DE INVERSIÓN Y ACTIVOS
DIVISIÓN DE CONTRATACIÓN DE ACTIVOS Y LOGÍSTICA

"2019, Año del Caudillo del Sur, Emiliano Zapata"

0116

Of N° 09 53 84 61 1CFJ/ **10236** /2019

Ciudad de México, a 24 de diciembre de 2019

Núm. De Contratación: **EPO-050-GYR019-N378-2019**

Instituto Potosino de Investigación Científica y Tecnológica, A.C.
Dr. Luis Antonio Salazar Olivo
Representante Legal
Presente

Por medio del presente, con fundamento en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos, y el Artículo 1° (primero), de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), se le notifica que mediante oficio **09 52 76 61 5300/2019001038** recibido el 23 de diciembre de 2019, el Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional de la Dirección de Innovación y Desarrollo Tecnológico del IMSS, comunicó la autorización para la contratación del, Servicio de Soporte Técnico y Operación de la Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube de IMSS y DRP, con esa empresa que representa.

La autorización indicada es por un monto mínimo de **$20,000,000.00** (Veinte millones de pesos 00/100 M.N.) y un monto máximo susceptible de ejercerse de **$50,000,000.00** (Cincuenta millones de pesos 00/100 M.N.) **los montos SI incluyen el Impuesto al Valor Agregado,** y una vigencia para la prestación del servicio a partir del 1° de enero y hasta el 29 de febrero del 2020, para ello la Coordinación de Sistemas de Infraestructura Tecnológica Institucional cuenta con el Dictamen de Disponibilidad Presupuestal Previo número **0000002733-2020.**

Asimismo se establece que los pagos se deberán calcular conforme a lo señalado en la propuesta económica la cual se da por reproducida en esta parte como si a la letra se insertara misma que se adjunta, y deberá formar parte integral del contrato que derive de la prestación del servicio.

De la consulta a la información publicada en el Sistema Electrónico de Información Pública Gubernamental, denominado CompraNet", sobre proveedores y contratistas sancionados con el impedimento para presentar propuestas o celebrar contratos no se encontró al proveedor arriba indicado.

La firma del contrato será a más tardar el **8 de enero de 2020** en la División de Contratos, debiendo entregar requisitados para la formalización los documentos que se anexan, sita en la Calle Durango número 291, Piso 10, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, Ciudad de México, lo anterior, de conformidad a lo establecido en el artículo 46 de la LAASSP.

Por último se informa que la vigencia de los servicios así como del contrato será a partir del 1° de enero y hasta el 29 de febrero del 2020.

Aprovecho la oportunidad para enviar un cordial saludo.

Atentamente,

Ing. Vicente Callejas Serrano
Titular

ANEXOS
DIVISION DE CONTRATOS

C.c.p.
Dr. Alberto Flavio Balderas Hernández.- Titular de la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
(*) Copias entregadas por SICGC
ACM

2019
EMILIANO ZAPATA

SIN TEXTO

Alberto Carbajal Maya

De:	Alberto Carbajal Maya
Enviado el:	martes, 24 de diciembre de 2019 03:23 p.m.
Para:	miriam@ipicyt.edu.mx
CC:	Eduardo Oropeza Ortiz; Vicente Callejas Serrano
Asunto:	AVISO DE ADJUDICACION
Datos adjuntos:	E378 LOGICA.pdf
Importancia:	Alta

0117

Seguimiento:	**Destinatario**	**Entrega**
	miriam@ipicyt.edu.mx	
	Eduardo Oropeza Ortiz	Entregado: 24/12/2019 03:23 p.m.
	Vicente Callejas Serrano	

Estimad@s

Asunto: Notificación Procedimiento de Contratación IMSS

1

Importancia: Alta

Buenas tardes:
En cumplimiento a lo establecido en los artículos 11 y 37 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público así como 35 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria, adjunto al presente en archivo PDF el oficio de aviso de adjudicación para la contratación número EPO-050GYR019-NB378-2019 del Servicio de Soporte Técnico y Operación de la Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube de IMSS y DRP.

Lo anterior para efectos de su notificación y efectos procedentes.
Saludos cordiales.

2

ANEXOS
DIVISION DE CONTRATOS

SIN TEXTO

	INSTITUTO MEXICANO DEL SEGURO SOCIAL **DIRECCIÓN DE ADMINISTRACIÓN** **UNIDAD DE ADQUISICIONES E INFRAESTRUCTURA** **COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS** **COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS**	**Contrato Número** **P0M0017**

ANEXO 3 (TRES)

"DOCUMENTO DE DESIGNACIÓN DE ADMINISTRADOR DEL CONTRATO"

ANEXOS
DIVISION DE CONTRATOS

EL PRESENTE ANEXO CONSTA DE **02** HOJAS INCLUYENDO ESTA CARÁTULA

SIN TEXTO

GOBIERNO DE MÉXICO | IMSS

DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO
Coordinación de Sistemas de Infraestructura Tecnológica Institucional

ACUSE

Oficio Nº 09 52 76 61 5300/2019000938

Ciudad de México, a 29 de noviembre de 2019

0126

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 Soporte Técnico y Operación de la Infraestructura Lógica para la Planeación y Pruebas de la Migración de la Nube de IMSS y DRP".**

Al respecto y a efecto de atender de manera oportuna las necesidades en materia de Tecnología de la Información y Comunicaciones del Instituto Mexicano del Seguro Social, les informo que el suscrito fungirá como **"Administrador del Contrato"**, con fundamento en lo dispuesto por los artículos 2 fracción V, 74, y 84 del Reglamento Interior del Instituto Mexicano del Seguro Social; numeral 4.17 y 5.3.15 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social, y conforme a lo previsto en el numeral 7.1.2., del Manual de Organización de la Dirección de Innovación y Desarrollo Tecnológico vigente, así como el *"ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias*, publicado en el Diario Oficial de la Federación el 23 de julio de 2018.

Sin otro particular por el momento, hago propicia la ocasión para enviarles un cordial saludo.

Atentamente,

Ing. Eduardo Oropeza Ortíz
Coordinador de Sistemas de Infraestructura Tecnológica Institucional adscrito a la DIDT

Y DESARROLLO TECNOLÓGICO
COORDINACIÓN DE SERVICIOS
02 DIC. 2019
10:09
OFICIALÍA DE PARTES

EOO/rvm

DID
SIN ANEXO

ANEXOS
DIVISION DE CONTRATOS

2019
EMILIANO ZAPATA

SIN TEXTO