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

Contrato para la prestación del Servicio de Comunicación para Enlaces de Criticidad Media y Normal del IMSS, Partida 2.- Servicio Administrado de Acceso a Internet, que celebran por una parte, el **INSTITUTO MEXICANO DEL SEGURO SOCIAL**, que en lo sucesivo se denominará **"EL INSTITUTO"**, representado en este acto por el **C. ALBERTO FLAVIO BALDERAS HERNÁNDEZ**, en su carácter de Apoderado Legal, y por la otra parte, la empresa denominada **OPERBES, S.A. DE C.V.**, a quien en lo sucesivo se le denominará **"EL PROVEEDOR"**, representada por los **CC. LUIS ALBERTO DE LA GARZA AGUIRRE** y **CÉSAR GERÓNIMO JIMÉNEZ CERVANTES**, en su carácter de Representantes Legales, 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 4° y 5° de la Ley del Seguro Social.

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

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

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

I.5.- Para el cumplimiento de sus funciones y la realización de sus actividades se requiere de la prestación del Servicio de Comunicación para Enlaces de Criticidad Media y Normal del IMSS, Partida 2.- Servicio Administrado de Acceso a Internet, 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 42061505 de conformidad con el Certificado de Disponibilidad Presupuestal Previo con número de solicitud 0000187152-2020, emitido por el Titular de la Coordinación de Servicios Administrativos de fecha 19 de mayo de 2020, documento que se agrega al **Anexo 1 (uno)** del presente contrato.

I.7.- Con fecha 31 de julio de 2020, en la Sesión Ordinaria número 07/2020, el Comité de Adquisiciones, Arrendamientos y Servicios (CAAS), dictaminó procedente el supuesto de excepción al procedimiento de Licitación Pública para llevar a cabo la contratación del Servicio de Comunicación para Enlaces de Criticidad Media y Normal del IMSS, Partida 2.- Servicio Administrado de Acceso a Internet, mediante Acuerdo número AC-39/SO-07/2020.

I.8.- Con fecha 07 de agosto de 2020, la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos, a través de la División de Contratación de Activos y Logística, mediante acta de adjudicación, notificó a **"EL PROVEEDOR"** la adjudicación del procedimiento de Adjudicación Directa Nacional número **AA-050GYR019-E132-2020**, con fundamento en lo dispuesto en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos, 26 fracción III, 26 Bis fracción I, 28 fracción I, 40 y 41 fracción III de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, los relativos de su Reglamento y demás disposiciones aplicables en la materia, como se detalla en el **Anexo 2 (dos)** del presente instrumento jurídico.

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

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

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

II.1.- Es una persona moral constituida de conformidad con las leyes de los Estados Unidos Mexicanos, según consta en la Escritura Pública número 16,515, de fecha 22 de marzo de 2007, pasada ante la fe del Licenciado Felipe Ignacio Vázquez Aldana Sauza, Titular de la Notaría Pública número 9 de Tlaquepaque, Jalisco, e inscrita en la Dirección del Registro Público de la Propiedad y de Comercio, de la misma Entidad, en el folio mercantil electrónico número 37737*1, con la denominación social "Operadora Bestel, S.A. de C.V.".

II.2.- Por escritura pública número 16,970, de fecha 03 de julio de 2007, pasada ante la fe del Licenciado Felipe Ignacio Vázquez Aldana Sauza, Titular de la Notaría Pública número 9 de Tlaquepaque, Jalisco, e inscrita en el Registro Público de la Propiedad y de Comercio de Guadalajara, Jalisco, en el folio mercantil electrónico número 37,737*1, se hizo constar el cambio de denominación social para quedar como "Operbes, S.A. de C.V.".

II.3.- Los CC. Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes, acreditan su personalidad en términos de la Escritura Pública número 25,706 de fecha 26 de febrero de 2018, pasada ante la fe del Licenciado Manuel Enrique Oliveros Lara, Titular de la Notaría Pública número 100 del Distrito Federal, 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.4.- Su objeto social conforme a sus Estatutos consiste, entre otros, en instalar, operar o explotar redes públicas de telecomunicaciones.

II.5.- Cuenta con los registros siguientes:

- Registro Federal de Contribuyentes número: **OPE070326DNA**.
- Registro Patronal ante **"EL INSTITUTO"** y **EL INFONAVIT** número: [redacted]

II.6.- Cuenta, al igual que su subcontratante, con el documento vigente expedido por el Servicio de Administración Tributaria (SAT), de opinión de cumplimiento de obligaciones fiscales en sentido positivo, de conformidad con el artículo 32 D del Código Fiscal de la Federación, así como a lo dispuesto por las Reglas 2.1.31 y 2.1.39 de la Resolución Miscelánea Fiscal para 2020, publicada el 28 de diciembre de 2019 en el Diario Oficial de la Federación, de los cuales presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

II.7.- Cuenta, al igual que su subcontratante, con el documento correspondiente vigente, expedido por **"EL INSTITUTO"** sobre el cumplimiento de sus obligaciones fiscales en materia de seguridad social, conforme al Acuerdo ACDO.SA1.HCT.101214/281.P.DIR dictado por el H. Consejo Técnico de **"EL INSTITUTO"** en la sesión ordinaria celebrada el 10 de diciembre de 2014, publicado en el Diario Oficial de la Federación el 27 de febrero de 2015 y su modificación publicada en el mismo de fecha 3 de abril de 2015, de los cuales presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

II.8.- Cuenta, al igual que su subcontratante, con el documento correspondiente vigente, expedido por el INFONAVIT en los términos del Acuerdo del H. Consejo de Administración del Instituto del Fondo Nacional de la Vivienda para los Trabajadores por el que se emiten las Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos, publicado en el Diario Oficial de la Federación el 28 de

junio de 2017, de los cuales presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

II.9.- Manifiesta bajo protesta de decir verdad, no encontrarse en los supuestos de los artículos 50 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

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

II.10.- Conforme a lo previsto en los artículos 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 107 de su Reglamento, **"EL PROVEEDOR"**, en caso de auditorías, visitas o inspecciones que practique la Secretaría de la Función Pública y el Órgano Interno de Control en **"EL INSTITUTO"**, deberá proporcionar la información relativa al presente contrato que en su momento se requiera.

II.11.- Reúne las condiciones de organización, experiencia, personal capacitado y demás recursos técnicos, humanos y económicos necesarios, así como con la capacidad legal suficiente para cumplir con las obligaciones que contrae en el presente contrato.

II.12.- Para efectos legales y de notificación relacionados con el presente contrato, señala como domicilio para oír y recibir toda clase de notificaciones y documentos, el ubicado en Avenida José Barros Sierra número 540, Torre 11, Piso 6, Colonia Lomas de Santa Fe, Demarcación Territorial Álvaro Obregón, Código Postal 01219, en la Ciudad de México; teléfono: (55) 4000 2418; 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 PROVEEDOR" se obliga a prestar el Servicio de Comunicación para Enlaces de Criticidad Media y Normal del IMSS, Partida 2.- Servicio Administrado de Acceso a Internet, cuyas características, cantidades, alcances y especificaciones se describen en los **Anexos 1 (uno)** y **2 (dos)** del presente instrumento jurídico, así como a las condiciones de la solicitud de cotización y Acta de Adjudicación del procedimiento del cual deriva el presente contrato.

SEGUNDA.- IMPORTE DEL CONTRATO.- El importe del presente contrato es por la cantidad de **$29,906,560.88 (VEINTINUEVE MILLONES NOVECIENTOS SEIS MIL QUINIENTOS SESENTA PESOS 88/100 M.N.)**, incluyendo el Impuesto al Valor Agregado (I.V.A.), de conformidad con los precios unitarios que se indican en el **Anexo 2 (dos)** del presente contrato.

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

TERCERA.- FORMA Y CONDICIONES DE PAGO.- Se efectuarán pagos a **"EL PROVEEDOR"** de conformidad con lo dispuesto en el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como lo establecido en los Términos y Condiciones que se agregan en el **Anexo 1 (uno)** del presente contrato.

El servicio descrito en el Anexo Técnico mismo que se integra en el **Anexo 1 (uno)** del presente contrato, está modelado con base en un esquema de pago unitario mensual, modalidad que permitirá el cálculo mensual del Comprobante Fiscal Digital por Internet (CFDI) que expida **"EL PROVEEDOR"** por cada uno de los conceptos del servicio que haya entregado durante el mes y estén funcionando de acuerdo al catálogo descrito con detalle en el Anexo Técnico mismo que se integra en el **Anexo 1 (uno)** del presente contrato. Para fines de facturación, **"EL INSTITUTO"** considerará a los meses con 30 (treinta) días, salvo aquellos casos en los que existan entregas parciales, es decir, sólo se considerarán para fines de facturación los días de servicio efectivamente prestados.

Bajo este esquema, **"EL PROVEEDOR"** debe reportar y solicitar a **"EL INSTITUTO"** el pago asociado al servicio que éste ha entregado y que esté funcionando conforme a las especificaciones descritas en el Anexo Técnico mismo que se integra en el **Anexo 1 (uno)** del presente contrato, y con estricto apego a las características y niveles de servicio que se requieren para cada rubro definido, sujeto a posibles deducciones por incumplimiento de los mismos, por lo que **"EL INSTITUTO"**, a través del Administrador del contrato, evaluará las condiciones de funcionalidad y operatividad de los servicios entregados por **"EL PROVEEDOR"** para que proceda el pago mensual que debe efectuarse por los mismos.

El detalle de las condiciones y procedimiento que habrá de seguirse para efectuar el pago de los servicios objeto de este contrato, se encuentra descrito a continuación:

"EL INSTITUTO" realizará por concepto del servicio, pagos mensuales dentro de los 20 (veinte) días posteriores a la presentación, validación y aceptación de los servicios por parte del Administrador del Contrato, así la documentación comprobatoria (entregables) y Acta de Aceptación del Servicio, con la que acreditará fehacientemente que se ha proporcionado el servicio a entera satisfacción de **"EL INSTITUTO",** y en estricto apego al procedimiento administrativo vigente en **"EL INSTITUTO"**. Dichos servicios deberán sustentarse mediante la entrega documental a **"EL INSTITUTO"**.

"EL PROVEEDOR" deberá contar previamente con los anexos 2 y 3 establecido en los Términos y Condiciones y Anexo Técnico mismo que se integran en el **Anexo 2 (dos)** del presente contrato, así como el acta de aceptación mensual elaborada y firmada por **"EL PROVEEDOR"** por la entrega del servicio avalada por el Administrador del Contrato, en la que

conste la aceptación de la prestación del servicio referido a entera satisfacción de **"EL INSTITUTO"**.

"EL PROVEEDOR" deberá entregar oportunamente el CFDI por los servicios devengados del mes, en la Coordinación Técnica de Servicios Administrativos de la Dirección de Innovación y Desarrollo Tecnológico, ubicada en Calle de Tokio número 80, 5º piso, Colonia Juárez, Demarcación Territorial Cuauhtémoc, Código Postal 06600, en la Ciudad de México, 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 pago de los servicios se efectuará en pesos mexicanos, a los 20 (veinte) días naturales posteriores a la entrega del CFDI y documentación comprobatoria que acredite la entrega de los servicios de conformidad con lo normado 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", en la División de Trámite de Erogaciones de la Coordinación de Contabilidad y Trámite de Erogaciones, dependiente de la Dirección de Finanzas, sita Calle Gobernador Tiburcio Montiel número 15, Colonia San Miguel Chapultepec, Demarcación Territorial Miguel Hidalgo, en la Ciudad de México, Código Postal 11850, de lunes a viernes en un horario de 9:00 a 14:00 horas, previa validación y autorización que para tal efecto realice el Administrador del contrato.

El CFDI que amparen bienes y 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 presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos" vigente.

"EL PROVEEDOR" deberá entregar los siguientes documentos:

- Original y copia del CFDI que expida **"EL PROVEEDOR"** a nombre de **"EL INSTITUTO"**, que reúna los requisitos fiscales, en la que se indiquen los servicios prestados, número de proveedor, número de contrato, número de fianza y denominación social de la Afianzadora; así como el reporte del servicio prestado, elaborado y firmado por el área usuaria y/o el Administrador del Contrato.
- Original y copia del presente contrato.
- Copia de la garantía de cumplimiento del contrato (póliza de fianza).
- En caso de aplicar, **"EL PROVEEDOR"** deberá de entregar nota de crédito a favor de **"EL INSTITUTO"** por el importe de la aplicación de la pena convencional por atraso o deductivas por la deficiencia del servicio.

"EL PROVEEDOR" deberá entregar a **"EL INSTITUTO"** la "Opinión de Cumplimiento de Obligaciones en materia de Seguridad Social" vigente y positiva. La "Opinión de Cumplimiento

de Obligaciones en materia de Seguridad Social" tendrá una vigencia de 30 (treinta) días naturales a partir del día de su emisión. En caso que **"EL PROVEEDOR"** no adjunte la "Opinión de Cumplimiento de Obligaciones en materia de Seguridad Social" o no esté vigente y/o sea negativa, no se recibirá su documentación, e informará que deberá obtener la citada Opinión, o en caso que sea negativa, que puede presentar aclaración o pagar sus créditos fiscales ante la Subdelegación que le corresponda o en caso que no esté vigente, que deberá obtenerla nuevamente.

"EL PROVEEDOR" deberá facturar mensualmente, por periodos mensuales vencidos de servicio, en los primeros diez días naturales del mes siguiente, debiendo entregar a **"EL INSTITUTO"** el (los) CFDI(s) correspondiente(s) al servicio, de acuerdo con lo siguiente:

A. **"EL PROVEEDOR"** entregará el CFDI a la Coordinación Técnica de Servicios Administrativos de la DIDT.
B. La Coordinación Técnica de Servicios Administrativos envía el CFDI a la Coordinación de Sistemas de Infraestructura Tecnológica Institucional.
C. La Coordinación de Sistemas de Infraestructura Tecnológica Institucional envía a la División de Telecomunicaciones el CFDI para su validación e integración del sustento documental.
D. El Administrador del contrato integra los respectivos sustentos documentales incluyendo las deducciones y penas convencionales conducentes.
E. La Coordinación de Sistemas de Infraestructura Tecnológica Institucional y/o la División de Telecomunicaciones, enviarán la documentación completa a la Coordinación Técnica de Servicios Administrativos para la gestión de pago.
F. La Coordinación Técnica de Servicios Administrativos entregará el CFDI a **"EL PROVEEDOR"**.
G. **"EL PROVEEDOR"** deberá ingresar su CFDI y documentación correspondiente al área de Trámite de Erogaciones para los trámites correspondientes.

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

"EL PROVEEDOR", para cada uno de los pagos que efectivamente reciba, de acuerdo con esta cláusula, deberá de expedir a nombre de **"EL INSTITUTO"**, el "CFDI con complemento para la recepción de pagos", también denominado "recibo electrónico de pago", el cual elaborará dentro de los plazos establecidos por las disposiciones fiscales vigentes y lo cargará en el portal de servicios a proveedores de la página de **"EL INSTITUTO"**.

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

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

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

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

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

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

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

"EL PROVEEDOR", durante la vigencia del presente contrato, se obliga a presentar a **"EL INSTITUTO"**, junto con el CFDI respectivo la constancia positiva y vigente emitida por el INFONAVIT y la "Opinión de cumplimiento de obligaciones en materia de seguridad social", vigente y positiva, la cual puede ser consultada a través de la página electrónica http://www.imss.gob.mx/tramites/cumplimiento-obligaciones, en los términos requeridos por **"EL INSTITUTO"**.

Los servicios cuya recepción no genere alta a través del SAI ni realice al PREI Millenium de manera electrónica, deberán contener la firma de recepción y de autorización para el trámite de pago de acuerdo a lo establecido en el "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación,

cancelación, operación y control de fondos fijos" vigente, así como el Acta de Entrega-Recepción.

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

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

En caso de que **"EL PROVEEDOR"** reciba pagos en exceso deberá reintegrar las cantidades pagadas en exceso más los intereses correspondientes, conforme a la tasa que establezca la Ley de Ingresos de la Federación, en los casos de prórroga para el pago de créditos fiscales.

Los intereses se calcularán sobre las cantidades en exceso y se computarán por días naturales desde la fecha de su entrega hasta la fecha en que se pongan efectivamente las cantidades a disposición de **"EL INSTITUTO"**.

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

El administrador del contrato llevará a cabo la valoración de la procedencia del pago por concepto de gastos no recuperables conforme a lo previsto en los artículos 101 y 102 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en relación con los artículos 38, 46, 54 Bis y 55 Bis, segundo párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, previa solicitud por escrito a **"EL PROVEEDOR"**, acompañada de los documentos siguientes:

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

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

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

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

CUARTA.- PLAZO, LUGAR Y CONDICIONES DE LA PRESTACIÓN DEL SERVICIO.- "EL PROVEEDOR" se obliga a prestar a **"EL INSTITUTO"** el servicio que se menciona en la Cláusula Primera del presente instrumento jurídico, conforme a lo establecido en el Anexo Técnico y en los Términos y Condiciones integrados en el **Anexo 1 (uno)** de este contrato, apegándose a las condiciones, alcances y características detalladas en la solicitud de cotización y acta de adjudicación del procedimiento del cual deriva el presente contrato, esta última se agrega en el **Anexo 2 (dos)**, y de acuerdo con lo siguiente:

PLAZO DE LA PRESTACIÓN DEL SERVICIO.- Serán a partir del día hábil siguiente al de la adjudicación y hasta el 31 de diciembre de 2020.

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

"EL PROVEEDOR" deberá cumplir en tiempo y forma con todas las actividades establecidas en el cronograma de actividades señalado en el **Anexo 2 (dos)** del presente contrato.

LUGAR DE LA PRESTACIÓN DEL SERVICIO.- "EL PROVEEDOR" se obliga expresamente a prestar el servicio en los sitios señalados en los apéndices del Anexo Técnico, que forma parte del **Anexo 2 (dos)** de este instrumento jurídico, y deberá activar los servicios conforme a lo señalado en el referido Anexo Técnico.

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

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

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

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

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

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

SÉPTIMA.- DE LAS NORMAS Y LICENCIAS.- Los servicios deberán cumplir con las Normas Oficiales Mexicanas y con las Normas Mexicanas, según proceda, y a falta de éstas, con las Normas Internacionales, de conformidad con lo dispuesto en los artículos 53 y 55 de la Ley Federal sobre Metrología y Normalización; en su caso, las normas de referencia o especificaciones técnicas que se señalan el artículo 67 de la Ley citada y cumplir con las características y especificaciones requeridas en el Anexo Técnico, Términos y Condiciones, mismos que se integran en el presente contrato como **Anexo 1 (uno)**.

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

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

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

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

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

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

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

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

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

DÉCIMA PRIMERA.- GARANTÍA DE CUMPLIMIENTO DEL CONTRATO.- "EL PROVEEDOR" se obliga a entregar dentro de los 10 (diez) días naturales siguientes a la firma del contrato, en términos de la fracción II del artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, una garantía de cumplimiento de todas y cada una de las obligaciones a su cargo derivadas del presente contrato, mediante fianza expedida por compañía autorizada en los términos de la Ley de Instituciones de Seguros y de Fianzas a favor del "Instituto Mexicano del Seguro Social" por un monto equivalente al 10% (diez por ciento) sobre el importe total adjudicado que se indica en la Cláusula Segunda del presente contrato, sin considerar el Impuesto al Valor Agregado (I.V.A.), en Moneda Nacional.

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

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

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

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

a) Se rescinda administrativamente el presente contrato.

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

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

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

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

DÉCIMA TERCERA.- PENAS CONVENCIONALES.- De conformidad con lo establecido en los artículos 45, fracción XIX, 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 95 y 96 de su Reglamento, la pena convencional aplicable a **"EL PROVEEDOR"**, será del 2.5% (dos punto cinco por ciento) sobre el valor de los servicios entregados en forma extemporánea, multiplicado por el número de días naturales transcurridos

desde el vencimiento hasta la entrega y conforme a lo señalado en el numeral 18 de los Términos y Condiciones incluidos en el **Anexo 1 (uno)** del presente contrato.

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

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

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

DÉCIMA CUARTA.- DEDUCCIONES.- Con fundamento en lo dispuesto en los artículos 53 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 97 de su Reglamento, **"EL PROVEEDOR"**, por la entrega parcial o deficiente del servicio, se hará acreedor a una sanción que se aplicará conforme al Tipo de Nivel de Servicio, Descripción del Nivel de Servicio, Métrica Objetivo Mensual, Deductiva Mensual Aplicable y Cómputo de la Deductiva, señalados en el numeral 19 de los Términos y Condiciones 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. El monto máximo de aplicación de las deducciones no podrán ser mayor al que resulte de aplicar el porcentaje de la garantía de cumplimiento del presente contrato.

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

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

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

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

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

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

1. Cuando no entregue la garantía de cumplimiento del presente contrato, a más tardar dentro de los 10 (diez) días naturales posteriores a la firma del mismo.
2. Cuando incurra en falta de veracidad total o parcial respecto a la información proporcionada para la celebración del presente contrato.
3. Cuando incumpla, total o parcialmente, con cualesquiera de las obligaciones establecidas en el presente contrato y sus anexos.
4. Cuando se compruebe que el servicio ha sido prestado con alcances y características distintas a las pactadas.
5. Cuando se transmitan total o parcialmente, bajo cualquier título y a favor de otra persona física o moral, los derechos y obligaciones a que se refiere el presente documento, con excepción de los derechos de cobro, previa autorización de **"EL INSTITUTO"**.
6. Si la autoridad competente declara el concurso mercantil o cualquier situación análoga o equivalente que afecte el patrimonio de **"EL PROVEEDOR"**.
7. Cuando de manera reiterativa y constante, **"EL PROVEEDOR"** sea sancionado por parte de **"EL INSTITUTO"** con penalizaciones y/o deducciones sobre el mismo concepto de los servicios que proporciona, o por ubicarse en los límites de incumplimientos previstos en la cláusula de penas convencionales y/o deducciones del presente instrumento.

8. Cuando se sitúe en alguno de los supuestos previstos en el artículo 50 de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público.
9. En el supuesto de que la Comisión Federal de Competencia Económica, de acuerdo con sus facultades, notifique a **"EL INSTITUTO"** la sanción impuesta a **"EL PROVEEDOR"** con motivo de la colusión de precios en que hubiese incurrido durante el procedimiento de contratación, en contravención a lo dispuesto en los artículos 9 de la Ley Federal de Competencia Económica y 34 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
10. Si **"EL PROVEEDOR"** no permite a **"EL INSTITUTO"** la administración y verificación a que se refiere la cláusula correspondiente del presente contrato.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PRÓRROGAS.- Asimismo, se podrán acordar prórrogas al plazo originalmente pactado por caso fortuito, fuerza mayor o por causas atribuibles a **"EL INSTITUTO"**, lo cual deberá estar debidamente acreditado en el expediente de contratación respectivo. **"EL PROVEEDOR"** puede solicitar la modificación del plazo originalmente pactado cuando se actualicen y se acrediten los supuestos de caso fortuito o de fuerza mayor.

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

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

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

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

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

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

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

de Procedimiento Administrativo, al Código Federal de Procedimientos Civiles y demás ordenamientos aplicables en la materia.

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

Previa lectura y debidamente enteradas **"LAS PARTES"** del contenido, alcance y fuerza legal del presente contrato, en virtud de que se ajusta a la expresión de su libre voluntad y que su consentimiento no se encuentra afectado por dolo, error, mala fe, ni otros vicios de la voluntad, lo firman y ratifican en todas sus partes, por duplicado, en la Ciudad de México, el **21 de agosto de 2020**, quedando un ejemplar en poder de **"EL PROVEEDOR"** y el restante en poder de **"EL INSTITUTO"**.

"EL INSTITUTO"
INSTITUTO MEXICANO DEL SEGURO SOCIAL

ADMINISTRADOR DEL CONTRATO

C. ALBERTO FLAVIO BALDERAS HERNÁNDEZ
Apoderado Legal

C. EDUARDO OROPEZA ORTÍZ
Coordinador de Sistemas de Infraestructura Tecnológica Institucional

"EL PROVEEDOR"
OPERBES, S.A. DE C.V.

C. LUIS ALBERTO DE LA GARZA AGUIRRE
Representante Legal

C. CÉSAR GERÓNIMO JIMÉNEZ CERVANTES
Representante Legal

RRSR/CPRD/LBGP/VER

SIN TEXTO

ANEXO 1 (UNO)

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

ANEXOS
DIVISIÓN DE CONTRATOS

EL PRESENTE ANEXO CONSTA DE **51** HOJAS INCLUYENDO ESTA CARÁTULA

SIN TEXTO

INSTITUTO MEXICANO DEL SEGURO SOCIAL

DIRECCION DE FINANZAS
COORDINACIÓN DE PRESUPUESTO E INFORMACIÓN PROGRAMÁTICA
CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL PREVIO

SOLICITUD: 0000187152 - 2020

Dependencia Solicitante:	D0009	Administración Central
	DID	Dir. Innovación y Desarrollo T
	09530007	M_OFICINAS ADMINISTRATIVAS
Descripción:	Servicio de Comunicación para Enlaces de Criticidad Media y Normal del IMSS, Partida 2: Servicio Adm	
Servicio:	SERVICIO DE TRANSMISION VOZ Y	
Fecha Impresión:	19/05/2020	Fecha Validación: 19/05/2020

	Importe	Cuenta
Total Comprometido (en pesos):	$ 38,000,000.00	42061505

COMPROMETIDO MENSUAL (en miles de pesos)

ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
0.0	0.0	0.0	0.0	0.0	0.0	9,500.0	4,750.0	4,750.0	4,750.0	4,750.0	9,500.0

Este documento de respaldo presupuestario se emite con base en la revisión efectuada en el Módulo de Control de Compromisos del Sistema Financiero PREI-Millenium, por lo que el monto señalado se encuentra comprometido para dar inicio a las gestiones de adquisición de bienes y servicios previo cumplimiento del marco normativo vigente, siendo responsabilidad del área solicitante el destino y aplicación de los recursos, lo anterior con fundamento en los artículos 35 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, 25 y 45 fracción III de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 24 y 46 fracción III de la Ley de Obras Publicas y Servicios Relacionados con las Mismas, 8°, 144 y 148 del Reglamento Interior del IMSS y el numeral 7.2.10 de la Norma Presupuestaria del IMSS.

CERTIFICADO PREVIO

CONTRATO PREI _____
CONTRATO IMSS _____

IMPORTE : $ 38,000,000.00
TREINTA Y OCHO MILLONES PESOS 00/100 MN

LEONARDO ALVARADO VELÁZQUEZ
Autorizó
TITULAR COORDINACIÓN DE SERVICIOS ADMINISTRATIVOS

ANEXOS
DIVISÍON DE CONTRATOS

SIN TEXTO

INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

SERVICIO DE COMUNICACIÓN PARA ENLACES DE CRITICIDAD MEDIA Y NORMAL DEL IMSS

ANEXO TÉCNICO
2020

ANEXOS

DIVISÍON DE CONTRATOS

Contenido

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
Ver. 1.0	18/03/2020	Documento inicial	Ing. José Carlos Aragón Herrera
Ver. 1.1	16/04/2020	Actualización documento	Ing. José Carlos Aragón Herrera
Ver. 1.5	20/05/2020	Actualización documento	Ing. José Carlos Aragón Herrera
Ver. 1.6	29/05/2020	Aprobación del documento	Ing. Eduardo Oropeza Ortíz

1. **Objetivo del documento**

Establecer las especificaciones técnicas, calendarios, arquitecturas y lineamientos para la contratación del Servicio de Comunicación para Enlaces de Criticidad Media y Normal del IMSS, el cual incluye los siguientes servicios:

- Partida 1: Servicio Administrado de Red Privada Virtual.
- Partida 2: Servicio Administrado de Acceso a Internet.

Clave CUCOP: 31600001

2. **Objetivo**

Contar con servicios administrados que presten al IMSS, de manera integrada y unificada, el suministro, configuración, operación, administración y soporte de Red Privada Virtual y Acceso a Internet, incluyendo el monitoreo y gestión.

El posible proveedor deberá ofertar, detallar y describir en su propuesta tanto la solución ofertada, como los alcances del servicio descritos en el presente documento, no solo repitiendo los compromisos, sino que también debe detallar las herramientas tecnológicas, recursos tecnológicos, humanos y materiales que utilizará para la prestación del servicio. En que el licitante no describa y detalle los componentes ofertados de la solución y que estos cumplan con los requerimientos del anexo técnico y sus apéndices, el Instituto considerará que no cumple con lo requerido en el presente documento.

Los servicios objeto de este contrato deberán cubrir las necesidades operativas de conectividad del IMSS en sus Unidades Médico-Administrativas del ámbito nacional en los nodos que se indican en los siguientes apéndices:

- Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual.
- Apéndice 2: Inventario de Nodos para el Servicio Administrado de Acceso a Internet.

3. **Vigencia del servicio**

El IMSS requiere los servicios objeto del presente procedimiento a partir del día siguiente de la notificación de la adjudicación y hasta el 31 de diciembre de 2020.

4. **Alcance**

El IMSS tiene la necesidad de contratar los servicios descritos en este anexo técnico para los inmuebles (nodos) definidos en los apéndices 1 y 2, los cuales están identificados por un número único (ID), el cual deberá ser respetado por los licitantes para efectos de diseño, documentación, propuesta técnica y eventualmente su operación.

Se hace de conocimiento del licitante que la volumetría que se proporciona en el catálogo de servicio, así como en los apéndices 1 y 2 es exclusivamente para efectos de cotización y no necesariamente reflejan los requerimientos del Instituto, por lo que dichas cantidades no se deberán considerar como las cantidades a contratar.

Cada licitante deberá cotizar precios unitarios por cada uno de los conceptos establecidos en el formato de propuesta económica. El contrato que resulte de este proceso de contratación será abierto y los servicios serán solicitados bajo demanda, la cantidad de servicios a

contratar se determinará por el presupuesto mínimo y máximo establecido, el uso de los servicios se determinará de acuerdo con las necesidades del Instituto.

5. **Catálogo de Servicios**

El catálogo de servicios de este anexo técnico resume todos los elementos de servicio que son considerados elementos de pago en el contrato correspondiente, y todos ellos guardan relación con servicios descritos en una o varias secciones de este anexo técnico. Los costos de los servicios solicitados en este anexo técnico serán pagados por el IMSS a mes vencido.

PARTIDA	CONCEPTO	ANCHO DE BANDA	MINIMO	MÁXIMO
PARTIDA 1	Enlace Satélite	1 Mbps	104	260
	Enlace Terrestre	6 Mbps	640	1600
	Enlace Terrestre	20 Mbps	24	60
	Enlace Terrestre	200 Mbps	24	60
	CENTRO DE MONITOREO	Cumplimiento de Niveles de Servicio	1	1
		Mesa de Servicios	1	1
		Información Ejecutiva	1	1
		Repositorio de Información	1	1

PARTIDA	CONCEPTO	ANCHO DE BANDA	MINIMO	MÁXIMO
PARTIDA 2	Servicios Administrados de Acceso a Internet para Nodo "Nube IMSS Digital"		1	1
	Servicios Administrados de Acceso a Internet para Nodo "CeNaTI DF"		1	1
	Servicios Administrados de Seguridad de Internet para el Nodo "CeNaTI DF"		1	1
	Servicios Administrados de Acceso a Internet para Nodo "CeNaTI Monterrey"		1	1
	Servicios Administrados de Seguridad de Internet para el Nodo "CeNaTI Monterrey"		1	1

Catálogo de Servicios

6. **Requerimientos técnicos**

Precios Unitarios

Los precios unitarios son los valores que cuantifican el costo de cada uno de los servicios que se incluyen en el catálogo de servicios de este anexo técnico. A cada concepto de servicio corresponde uno y solo un precio unitario. El licitante debe tomar en cuenta que los precios unitarios serán permanentes e inamovibles a lo largo de la vigencia del contrato.

Arquitectura de referencia

El siguiente esquema resume, de manera muy sucinta y meramente referencial, los grandes flujos de interconexión existentes actualmente en el IMSS.

Como puede observarse existen 2 nubes de conectividad en la Red Privada Virtual del IMSS que atiende aproximadamente a 3,000 nodos, entre los que se encuentra toda clase de inmuebles asociados a la operación del Instituto. Más detalles de los tipos de inmueble y su orientación de negocio pueden revisarse en el Apéndice 1 de este documento.

El diagrama 1 establece de manera muy general, la arquitectura en la que actualmente el IMSS opera. El servicio a contratar para la Partida 1 en el presente procedimiento se encuentra acotado con líneas punteadas.

Es importante mencionar que los inmuebles contemplados en esta contratación no son necesariamente la totalidad de inmuebles en los que el IMSS opera.

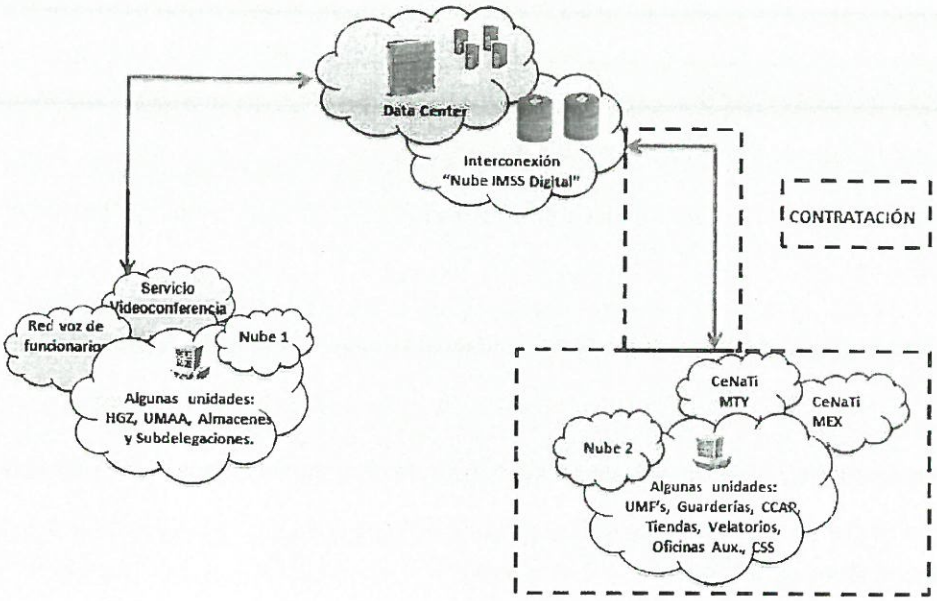


Diagrama 1

El diagrama 2 establece de manera muy general, la arquitectura en la que actualmente el IMSS opera. El servicio a contratar para la Partida 2 en el presente procedimiento se encuentra acotado con líneas punteadas.

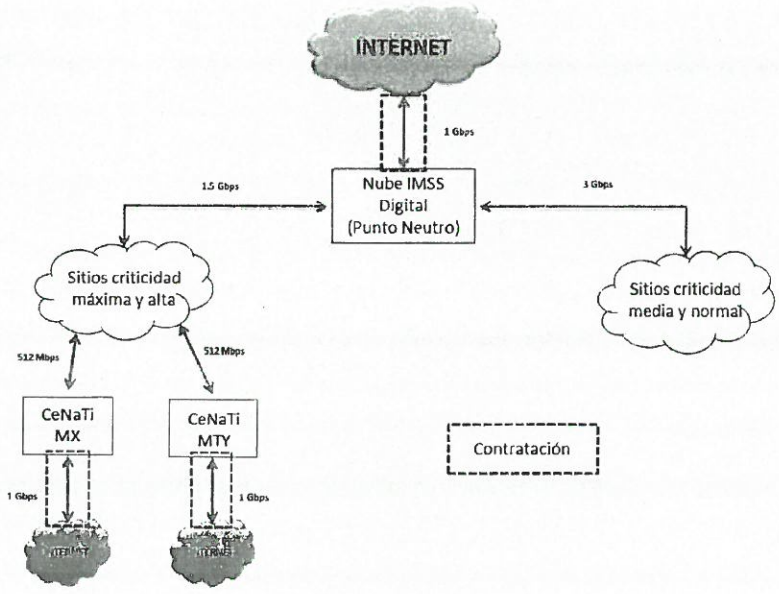


Diagrama 2

7. Especificaciones técnicas

PARTIDA 1

El servicio objeto del presente contrato se prestará a partir del día siguiente de la notificación de la adjudicación y hasta el 31 de diciembre de 2020.

7.1 Servicio Administrado de Red Privada Virtual

El Instituto requiere una red privada que proporcione el servicio a los sitios señalados en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual", la cual ya sea de manera terrestre o satelital, deberá proporcionar lo siguiente:

(i) El servicio de red de transporte de datos para el tráfico de datos que genere el Instituto, así como ofrecer la infraestructura necesaria e instalación de esta para proporcionar dicho servicio.

(ii) El mantenimiento y soporte a la infraestructura de comunicaciones del servicio que corresponda a los componentes que el proveedor utilice para la entrega del mismo, el cual será de acuerdo a su estrategia de mantenimiento correctivo y soporte para garantizar los niveles de servicio solicitados.

(iii) Un centro de monitoreo para los servicios señalados en el punto (i) que incluya los siguientes servicios y/o actividades:
- Cumplimiento de Niveles de Servicio.
- Mesa de Servicios.
- Información Ejecutiva.
- Repositorio de Información.

La descripción técnica del servicio se encuentra desarrollada de la siguiente forma en este anexo técnico:

A. Conformación, descripción, equipamiento y necesidades de los sitios.
B. Consideraciones del listado de sitios.
C. Descripción técnica de los enlaces para el servicio.
   i. Requisitos técnicos de los enlaces satelitales.
   ii. Requisitos técnicos de los enlaces terrestres.
D. Centro de Monitoreo.
   i. Cumplimiento de Niveles de Servicio
   ii. Mesa de Servicios
   iii. Información Ejecutiva
   iv. Repositorio de Información

A. CONFORMACIÓN, DESCRIPCIÓN, EQUIPAMIENTO Y NECESIDADES DE LOS SITIOS

El proveedor deberá de prestar el servicio para los sitios señalados en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual", por lo cual el proveedor de forma enunciativa más no limitativa deberá proporcionar, configurar y realizar todas las actividades inherentes a la prestación del servicio.

Es importante señalar, que durante la vigencia del contrato el Instituto podrá agregar o disminuir la cantidad de sitios terrestres y satelitales.

B. CONSIDERACIONES DEL LISTADO DE SITIOS

Dentro de su propuesta técnica, el posible proveedor deberá expresar de manera clara y precisa el tipo de enlace que oferta para cada sitio relacionado en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual". Para este fin, el posible proveedor deberá requisitar la información solicitada para cada sitio relacionado en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual".

A continuación, se ejemplifica la información que deberán proporcionar en el citado anexo:

Id.	SITIO	OFERTA SERVICIO MPLS (SI/NO)	TIPO ENLACE	ENTREGA MPLS EN F.O. O COBRE	COMENTARIOS (TEXTO LIBRE)
1-xxxx					

Dónde:
Id. = Identificador del sitio proporcionado por el Instituto en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual".
Sitio = Es el nombre del sitio identificado en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual"
Oferta servicio MPLS = (SI/NO) Información que deberá proporcionar el posible proveedor.
Tipo de enlace = Satelital o terrestre
Entrega MPLS en F.O. o cobre = Información que deberá proporcionar el posible proveedor.
Comentarios (texto libre) = Información que deberá proporcionar el posible proveedor.

C. DESCRIPCIÓN TÉCNICA DE LOS ENLACES PARA EL SERVICIO

Requisitos técnicos de los enlaces satelitales.
Para los enlaces satelitales, el servicio incluye, todos los elementos, recursos humanos, materiales y físicos para las actividades de continuidad del servicio, así como proporcionar todos los elementos necesarios para el servicio.

Para lograr tiempos de respuesta óptimos y cumplir con los requerimientos de latencia mínimos solicitados en este anexo técnico, el posible proveedor deberá contar con la conexión directa de su POP de MPLS con el telepuerto de la solución satelital, por lo que deberá entregar en su propuesta técnica la documentación que avale el tipo de conexión y detalle de anchos de banda.

El Instituto a través del Administrador del Contrato durante la vigencia del contrato, podrá solicitar la reubicación de hasta el 10% de los enlaces satelitales a otras ubicaciones de acuerdo con las necesidades que durante la vigencia del servicio el Instituto requiera, lo anterior sin costo adicional para el Instituto.

Requisitos generales para los enlaces satelitales:

- Disponibilidad del servicio de 98.89% mensual (ver tabla 2, Niveles de servicios)
- Contar con un telepuerto satelital dentro del territorio nacional donde se recibirán, administrarán y operarán los enlaces satelitales.
- Deberá ser un sistema satelital bi-direccional.
- Los equipos de telecomunicación deberán ser monitoreables remotamente.
- Los equipos de telecomunicación deberán ser configurables remotamente.

- El proveedor deberá proporcionar los servicios de conectividad satelital bidireccional de banda ancha con velocidad de recepción y transmisión de 1Mbps / 1Mbps en canal de retorno con sobresuscripción no mayor de 30 a 1, compatible con estándares de comunicación IP, el cual cuente con codificación avanzada, técnicas de corrección de errores y funciones de seguridad que se utilicen para permitir una transmisión confiable y segura así como mecanismos de aceleración TCP/IP incorporados que permitan mejorar la experiencia del usuario. Así como una latencia máxima de 750 ms, con pérdida de paquetes menor al 1%.
- Aceleración y optimización incorporada TCP/IP para comunicación vía satélite.
- Modulación variable para garantizar la disponibilidad de los enlaces.
- Modulación variable: QPSK, 8PSK, 16APSK, 32APSK (o superior).
- El proveedor podrá calcular las características de las portadoras de retorno con base en el cálculo de enlace. Sin embargo, se deberán incluir canales dinámicamente adaptativos a la modulación y el FEC dependiendo de las condiciones de operación de las estaciones terrenas remotas.
- FEC RATE (DVB-S2): 1/4,1/3,2/5,1/2,3/5,2/3,3/4,4/5,5/6,8/9,9/10.
- Consumo de potencia menor a 20 watts (lo anterior refiriéndose al radio de unidad exterior ODU).
- Rango de frecuencia de transmisión: Banda Ku.
- Los equipos deberán soportar vientos iguales o superiores a 70 km/h en operación.
- Temperatura de operación de ODU de -40 a 50 grados centígrados.
- Adaptabilidad portadora de retorno; soportar los modelos: AUPC, canales dinámicos y modulación/FEC. Se podrá modificar las características de la portadora de retorno, únicamente cuando la señal sea con características iguales o superiores a las antes solicitadas.
- Soportar algoritmos o herramientas que permitan incrementar la eficiencia propia de los códigos de corrección de error y mejorar la relación señal a ruido, así como ajustar dinámicamente los códigos de error y modulación de las portadoras ascendentes y descendentes a fin de mantener la disponibilidad de los enlaces durante variaciones ambientales adversas como lluvia, polvo o nieve de tal manera que se obtenga el mejor desempeño global en la red.
- Portadora de entrada con capacidad de modulación QPSK, 8APSK, con capacidad de hasta 6 Mbps.
- Esquema de acceso estándar al satélite en antena maestra (Tele Puerto): DVB-S2 con soporte a modulaciones de hasta 32APSK Y ACM, la modulación deberá de ajustarse de manera dinámica de acuerdo al ACM. Mientras que el QoS deberá ajustarse de manera dinámica al tipo de tráfico y/o aplicativos.
- La marca y el modelo del equipo de telecomunicaciones son a consideración del posible proveedor, siempre y cuando cumpla con lo descrito en las especificaciones del servicio.

El servicio mediante enlaces satelitales incluye:

- Antenas fijas para los sitios con un diámetro de 1.2 mts hasta 1.8 mts dependiendo de las facilidades del inmueble de acuerdo al "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual" y todo el aditamento necesario para su correcto funcionamiento, el proveedor deberá garantizar que dicha antena sea resistente al agua, al polvo y a condiciones adversas.
- El proveedor deberá instalar las antenas satelitales fijas junto con todos los aditamentos necesarios para su funcionamiento en los techos de los inmuebles de las unidades, el proveedor tendrá que realizar cableado para conectar la antena con el módem satelital, mismo que el proveedor deberá instalar en el interior de inmueble. Los permisos de acceso a los inmuebles para realizar estas tareas serán coordinados con el Instituto.
- Radios y/o módem, así como todo el equipamiento aplicable para el correcto funcionamiento del enlace satelital.
- Todos los cables necesarios para el correcto funcionamiento del enlace satelital.

- Instalación en caso de ser necesario, de un sistema de tierra física independiente.
- El servicio debe permitir el transporte de datos para los aplicativos del Instituto.
- El proveedor deberá proporcionar la configuración inicial y puesta a punto, así como las licencias y software que se requiera para brindar el servicio mediante enlace satelital.
- El servicio deberá contar con las últimas versiones liberadas por el fabricante así como el release de software, firmware y otros relacionados, éstas deberán ser actualizadas en los equipos de telecomunicaciones durante la vigencia del contrato por el proveedor previa coordinación con personal del Instituto y sin costo adicional para el mismo.
- Mecanismos y/o seguros contra el robo de equipos y daños que éstos pudieran sufrir por vandalismo, fenómenos naturales, accidentes, inestabilidad eléctrica o cualquier otra causa, será responsabilidad del proveedor restablecer el servicio para cumplir el nivel de servicio indicados en la tabla 2 "Niveles de servicio". Cabe señalar, que por accidente se entiende cualquier eventualidad que interrumpa la continuidad del servicio.
- El proveedor deberá realizar todas las reparaciones que sean necesarias para garantizar la impermeabilidad de las paredes y azoteas (lozas) en los lugares que realice perforaciones para la sujeción de los equipos. De igual forma el proveedor deberá realizar todas las reparaciones que sean necesarias para restaurar a su estado original cualquier daño que cause derivado de la instalación de los equipos propuestos para la prestación del servicio. En caso de que el proveedor no realice las reparaciones a las que hace referencia en este punto, se penalizará con una cantidad de $10,000.000 (diez mil pesos 00/100) M.N. por cada sitio que no esté reparado al momento de recibir el servicio efectivamente prestado, así como al momento de que concluya el contrato.
- Ningún sitio cuenta con sistemas de acondicionamiento de la temperatura y humedad ambientales, por lo que el posible proveedor deberá de tomar esto en cuenta para la selección de los equipos que integrarán su propuesta, en las que establezca condicionantes de temperatura o humedad.
- El proveedor es responsable de realizar las adecuaciones y todos los insumos y accesorios necesarios que permitan instalar adecuadamente los equipos y poner en operación el servicio y garantizar su continuidad: charolas o sujeción en pared, tornillos, cables, conectores, cinturones de plástico (cinchos), etc.
- El proveedor podrá imputar fallas del servicio por cortes en el suministro de energía eléctrica.
- En caso que una antena se mueva o se obstruya la línea de vista con letreros u ocurra un acontecimiento semejante a los descritos, el proveedor tiene la responsabilidad de repararlos cumpliendo con los niveles de servicio descritos en este anexo técnico.
- El personal del proveedor deberá portar en todo momento una identificación dentro de los sitios del Instituto durante el desarrollo de los trabajos necesarios para prestar el servicio.

Requisitos técnicos de los enlaces terrestres.

El servicio a través de enlace terrestre consiste en la interconexión vía MPLS (RFC 2547 de la IEFT) a través de enlaces digitales, lo cual permitirá intercambiar información a través de aplicativos propios del Instituto (voz, datos, video y colaboración).

Para los enlaces terrestres, el servicio incluye todos los elementos, recursos humanos, materiales y físicos para coordinar las actividades de continuidad del servicio, así como proporcionar todos los elementos necesarios para proporcionar el servicio, así como todo el equipo necesario, con el fin de proporcionar los servicios de conectividad con el ancho de banda solicitado en los sitios.

El posible proveedor debe contar con una red privada o backbone nacional propia.

El posible proveedor deberá tener **cobertura terrestre al menos del 85% de los sitios listados en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual"** con el fin de minimizar los tiempos de atención e integración de los servicios. Para los sitios terrestres no se aceptarán soluciones satelitales, inalámbricas o microondas, por lo que la solución propuesta por el posible proveedor deberá ser únicamente por medio de fibra óptica o cobre.

Para el caso de nuevos requerimientos, el servicio incluye un equipo terminal (router), el cual deberá contar con al menos 1 slot disponible para ampliar la capacidad de puertos de interconexión en caso de requerirse. y todos deberán ser de la misma marca, no se aceptan soluciones con más de una marca y deberá ser administrado y monitoreado de manera remota a través del centro de monitoreo que más adelante se especifica en este anexo técnico. La marca y el modelo del equipo de telecomunicaciones son a consideración del posible proveedor, siempre y cuando cumpla con lo descrito en las especificaciones del servicio.

El servicio mediante enlaces terrestres incluye:

- La red privada del proveedor debe operar las 24 horas del día, los 7 días de la semana, los 365 días del año, de manera que cumpla con una disponibilidad en su backbone de al menos 98.89% mensual (ver tabla 2, Niveles de servicio).
- La red privada del proveedor debe soportar una conectividad conocida como any-to-any, asimismo deberá soportar el direccionamiento IP que se designe y permitir la designación de subredes para conformar la segmentación física o lógica según sea el caso y soportar la configuración de NAT (Network Address Translation) y/o PAT (Port Address Translation). También deberá contar con tiempos de latencia entre dos nodos de su backbone con valores inferiores a los 50 milisegundos considerando una trayectoria de ida y vuelta (round-trip), mientras que los valores del Jitter deben encontrarse por debajo de los 50 milisegundos en una dirección y pérdida de paquetes menores al 1%.
- El servicio deberá operar con una red privada sectorial, por lo que la comunicación a cada uno de los sitios que conformen la red será de forma directa, es decir; no deberá pasar por ningún sitio central de cualquier otra red.
- El servicio deberá contar con las últimas versiones liberadas por el fabricante, así como el release de software, firmware y otros relacionados, éstas deberán ser actualizadas en los equipos de telecomunicaciones durante la vigencia del contrato por el proveedor previa coordinación con personal del Instituto y sin costo adicional para el mismo.
- El Instituto podrá solicitar durante la vigencia del contrato, la reubicación de hasta el 10% de los enlaces terrestres a otras ubicaciones, lo anterior sin costo adicional para el Instituto.
- El posible proveedor deberá tomar en cuenta que el Instituto podrá solicitar enlaces terrestres de hasta 20 Mbps para poder soportar las aplicaciones futuras de telemedicina y mayor transferencia de información.
- El personal del proveedor deberá portar en todo momento una identificación dentro de los sitios del Instituto durante la prestación del servicio.

D. CENTRO DE MONITOREO

El servicio incluye un centro de monitoreo, el cual deberá controlar de forma permanente el grado, la calidad de la entrega y el soporte de los requerimientos que incluye el servicio mediante las siguientes actividades:

i. Cumplimiento de Niveles de Servicio.
ii. Mesa de Servicios.
iii. Información Ejecutiva.
iv. Repositorio de Información.

El centro de monitoreo incluye todos los recursos humanos, materiales, la metodología de entrega, soporte; manuales y procedimientos operativos necesarios para la provisión de las actividades anteriores. Cabe aclarar que las herramientas antes señaladas no necesariamente tienen que ser de la misma marca.

Requisitos técnicos del Centro de Monitoreo.

- El centro de monitoreo deberá ser accesible desde cualquier acceso vía Internet/IP por HTTP/WEB en tiempo real y a toda hora, permitiendo de igual forma realizar el seguimiento de reportes de fallas por el personal del Instituto.
- El proveedor deberá contar con una sola herramienta de monitoreo, por lo que en caso de tener diferentes mesas de servicio (satelital y terrestre), deberá comprobar que se cuenta con la integración correspondiente.
- Los usuarios que tendrán acceso al centro de monitoreo serán definidos en las mesas de planeación con el proveedor.
- El centro de monitoreo no deberá tener un límite de usuarios.
- El centro de monitoreo será provisto bajo el entorno de los siguientes estándares internacionales: ISO 20000, ISO 9001 e ISO 27001. El posible proveedor deberá demostrar que cuenta con estas certificaciones y deberá entregar copia simple del certificado que lo compruebe.
- El centro de monitoreo deberá de tener un nivel de servicio del 98.89% de disponibilidad mensual (ver tabla 2, Niveles de servicio) y deberá estar disponible para uso del Instituto a partir del día que entre en operación el primer sitio.
- Las herramientas del centro de monitoreo deberán estar alojadas en un centro de datos de alta disponibilidad y alta seguridad, mismo que deberá contar al menos con las siguientes certificaciones:
  a) ISO 9001:2008 o superior
  b) ISO/IEC 27001:2005
  c) ISO/IEC 20000-1:2011
- El centro de monitoreo deberá localizarse en inmuebles diferentes a los del Instituto con la redundancia correspondiente al nivel de servicio solicitado, el proveedor deberá demostrar que el centro de monitoreo cuenta con infraestructura redundante como son acometidas eléctricas, plantas de emergencia, UPS y sistemas antiincendios. Dichas mplaciones serán visitadas por lo menos una vez al año, durante cualquier etapa de la prestación del servicio por el Instituto para su evaluación y verificar el cumplimiento de las funciones del citado centro.
- De lo anterior, el posible proveedor deberá demostrar mediante manifiesto firmado por el representante legal que el centro de monitoreo cumplirá con las especificaciones solicitadas en este anexo técnico.
- El Instituto se reserva el derecho de efectuar el monitoreo del servicio de manera directa o a través de un tercero, previa firma de los "OLA's" Acuerdos Operacionales correspondientes. En su caso, el monitoreo del tercero contribuirá como una fuente de datos adicional en la determinación del cumplimiento de los niveles de servicio, así como en información complementaria para el cálculo de las deductivas y penas convencionales correspondientes, señaladas en los Términos y Condiciones.

D.i. Cumplimiento de Niveles de Servicio

El proveedor debe proporcionar el cumplimiento de los niveles de servicio de los servicios de comunicación, el cual debe ser proporcionado a través de herramientas graficas especializadas y con apego a las mejores prácticas de ITIL.

El proveedor deberá ofrecer una interface de verificación de los niveles de servicio que tenga la capacidad de ser consultada en línea vía web, sin límite de usuarios, ya sea vía internet o a través de una red privada y que además cuente con indicadores gráficos de rendimiento global y por grupos de inmuebles mostrando niveles de servicios y resumen de fallas catalogadas.

El cumplimiento de niveles de servicio deberá asimismo cumplir con los siguientes requerimientos:

- Operar los 365 días del año, los 7 días de la semana, las 24 horas del día.
- Tener un nivel de disponibilidad del 98.89% garantizado, a través de los siguientes conceptos de acuerdo con el diseño: Equipamiento de cómputo, almacenamiento y de red redundante tanto en fuentes como en procesadores.
- Contar con planta de emergencia y UPS en las instalaciones del proveedor donde se encuentre el centro de monitoreo, para garantizar la disponibilidad de la solución.
- Recolectar muestras o lecturas de indicadores de rendimiento diarias.
- Capacidad de medir en línea y en tiempo real el comportamiento operativo de los componentes de comunicaciones de la solución. El comportamiento operativo versará sobre los componentes como el CPU, memoria, ancho de banda de los equipos de telecomunicaciones.
- Deberá incluir una herramienta de generación de reportes en línea para la toma de decisiones relacionadas con el tráfico de la red, niveles de servicio e indicadores de rendimiento de la red.
- Los indicadores de rendimiento son enfocados a los equipos de telecomunicaciones de los cuales se pude extraer información del CPU, memoria, ancho de banda latencia y paquetes perdidos.
- Considerar alarmas interactivas para cualquier evento que rebase los umbrales definidos en las mesas de planeación con el proveedor y que pongan en riesgo la operación de la red objeto del servicio con aviso vía SMS y/o correo electrónico, tanto para personal del Instituto como para personal del proveedor, quien tendrá la responsabilidad de atender de manera oportuna los incidentes con la finalidad de cumplir con los niveles de servicio solicitados en el presente anexo técnico. Los avisos al personal del Instituto se definirán de manera conjunta con el proveedor en las mesas de planeación.
- Generar información y reportes para la planeación de capacidades de los servicios de comunicación de acuerdo a lo solicitado por el Instituto en las mesas de planeación.
- Manejar vistas completas con un sistema visual de alarmas representando en forma gráfica al menos los siguientes indicadores de niveles de servicio:
    - Disponibilidad de servicio por sitio y por equipo.
    - Latencia por sitio.
    - Pérdida de paquetes por sitio.
    - Paquetes con error de trama por sitio.
    - Consumos de instancias de procesador, memoria y cualquier otro indicador permitido por el tipo de MIB (Management Information Base).
    - Consumo de ancho de banda por sitio.
    - Medir el comportamiento del tráfico clasificado por clase de servicio monitoreando, retardos, disponibilidad, paquetes perdidos por cada enlace.

El proveedor será responsable de realizar los estudios de desempeño de la red y de las capacidades diarias a través de la medición del tráfico generado de entrada y salida y de la utilización de los equipos activos de comunicaciones, por lo que debe contar con herramientas que permitan generar, verificar y almacenar estadísticas del desempeño, capacidad y utilización de los componentes de soporte del servicio.

Los registros generados en el proceso de verificación de los niveles serán utilizados para apoyar al Instituto en el proceso de validación de los niveles de servicio que se contratarán con el posible proveedor.

Deberá ser capaz de gestionar los centros de costos por cada sito del Instituto, es decir llevar a cabo el análisis de desempeño de la red y de las capacidades diarias a través de la medición del tráfico generado de entrada y salida, así como de la utilización de los equipos de comunicaciones por cada sitio.

D.ii. Mesa de Servicios

El servicio a través del centro de monitoreo incluye una mesa de servicios que será el único punto de contacto para la atención de los usuarios del Instituto y del tercero que el IMSS defina para la vigilancia del cumplimiento de los niveles de servicio.

La mesa de servicios del proveedor será la responsable de detectar, comunicar y reparar cualquier falla de los servicios de comunicación, en tiempo y forma para poder cumplir con los niveles de servicios establecidos en este anexo técnico.
El posible proveedor deberá presentar los procedimientos probados y procesos certificados ISO 9001, ISO 20000 e ISO 27001 que actualmente utiliza en los siguientes puntos que a la vez serán su responsabilidad el dar cumplimiento durante la vigencia del contrato:

- Registro y escalación de los reportes de falla y de requerimientos que usará para la operación del servicio, considerando que deberán ser atendidos por un operador, el cual se encargará de darle seguimiento y solución en su caso hasta el cierre definitivo del reporte, ya sea mediante soporte a primer nivel como de escalación a terceros.
- Recepción en primera instancia de los reportes de incidentes detectados por el Instituto y/o del tercero que el IMSS defina para la vigilancia del cumplimiento de los niveles de servicio en forma reactiva, es decir aquellas fallas que no fueron detectadas de manera oportuna.
- Coordinación de uno o más proveedores que se encuentren involucrados en la prestación del servicio en un determinado incidente.
- Conteo de los tiempos de inicio y término de los incidentes.
- Revisión con el Instituto y/o del tercero que el IMSS defina para la vigilancia del cumplimiento de los niveles de servicio, que las funcionalidades del servicio se encuentren operando completamente después de un incidente.
- De acuerdo a las mejores prácticas, se deberá realizar el almacenamiento en una base de datos de la información correspondiente al proceso de resolución de incidentes.
- Notificación al Administrador del Contrato, desde el inicio hasta la finalización de un evento de falla vía los siguientes medios posibles: correo electrónico, vía telefónica, envío de mensajes SMS, notificador de la herramienta de mesa de servicios.
- Entregar al Administrador del Contrato con una periodicidad mensual, un reporte de los incidentes, sus tiempos de atención y caídas de los enlaces.

El posible proveedor deberá entregar como parte de su propuesta técnica, el modelo que utiliza para el manejo de los diferentes perfiles que intervienen en sus procesos y la organización de su mesa de servicios, lo anterior, de forma enunciativa y no limitativa:

- Matriz de escalación: El posible proveedor deberá entregar en su propuesta técnica el modelo de matriz de escalación que utilizará en caso de resultar adjudicado para controlar los servicios de conectividad que recibirá el Instituto durante la vigencia del contrato.
- El proceso de atención a incidentes: La mesa de servicios deberá incluir los campos necesarios para la óptima clasificación y almacenamiento de los reportes que serán acordados junto con el Instituto y estos deberán apegarse a las mejores prácticas como los KPI de ITIL.

El posible proveedor deberá presentar en la propuesta técnica la metodología, formatos y procedimientos que usará para medir en forma mensual la satisfacción del servicio que recibe el Instituto y deberá mostrar las estrategias que llevará a cabo para lograr un proceso de mejora continua.

D.iii. Información Ejecutiva

El proveedor además de entregar en forma periódica o a petición expresa por parte del Instituto, los reportes electrónicos de los resultados de su actividad; Deberá contar con información ejecutiva a través de un portal en Internet, basado en la administración de indicadores claves de desempeño.

La información ejecutiva deberá proporcionar la facilidad de realizar consultas personalizadas de la información generada global y por sitio, así como sus combinaciones y permitir su importación a formato electrónico e impresión en forma local.

A través del portal, permitirá consultas simultáneas de múltiples usuarios. El formato detallado de la información se definirá, en reunión de trabajo como máximo treinta días hábiles después de la notificación de fallo.

El portal, al menos, deberá presentar en tiempo real y de manera sencilla la interpretación de las variables monitoreadas, tales como: porcentajes de tráfico de diferentes clases vs prioridad de los sitios, reporteo por sitio por tipo de paquete, los cuales combinarán variables de SLA (latencia, jitter, perdida de paquetes, etc.) por cada grupo de prioridad de sitios y asociarlo a su precio mensual. Para lo anterior, el sistema y la arquitectura queda a consideración del posible proveedor.

Asimismo, los reportes deberán tener la capacidad de entregar la siguiente información:

- Usuarios que reportan incidencias.
- Reparaciones realizadas (y tiempo invertido en las reparaciones).
- Número de atenciones telefónicas realizadas durante el año o periodo especifico.
- Disponibilidad física de equipos y medios.
- Niveles de servicio.
- Tipo de tráfico por puertos y protocolos.
- Retardo/Latencia.
- Reportes de dispositivo específicos por nodo del servicio.
- Los reportes deberán permitir seleccionar el periodo (por día, semana, mes, año, de fecha a fecha) y/o por grupo de nodos.
- Reportes de utilización del ancho de banda de salida y entrada
- Reportes de tendencias, por tendencia se deberá entender a las proyecciones del comportamiento de la red con base en su comportamiento histórico.
- Proveer en forma mensual estadísticas de las incidencias.
- Caídas de los enlaces y su duración por sitio y globales.

D.iv. Repositorio de Información

Será responsabilidad del proveedor proporcionar al Instituto un repositorio de información que cumpla con las siguientes funcionalidades.

El proveedor será responsable de contar con herramientas y procedimientos que garanticen la continuidad, seguridad e integridad de la información almacenada durante la vigencia del contrato.

La información por sitio deberá ser almacenada en forma centralizada durante la vigencia del contrato en un repositorio físico de información, con capacidad de almacenamiento suficiente, en las instalaciones del proveedor que deberá contener al menos:

- Métricas de los SLA.

- Mantenimientos correctivos.
- Administración de cambios. Entendiéndose como administración de cambios al proceso basado en ITIL o ISO 20000 que tiene la finalidad de controlar el ciclo de vida de todos los cambios y teniendo como objetivo principal viabilizar los cambios beneficiosos con un mínimo de interrupciones en la prestación de servicios de TI.
- Base de datos de configuraciones. Por base de datos de configuraciones se deberá entender como una base de datos que contiene detalles relevantes de cada elemento de configuración y de la relación entre las mismas, incluyendo equipo físico, software y la relación entre incidencias, problemas, cambios y otros datos del servicio.
- Base de datos de capacidades.
- Base de datos de problemas.
- Reportes de monitoreo de indicadores y niveles de servicio.
- Reportes de la mesa de servicios.
- Respaldos de configuraciones de Servidores y equipos CPE (Client Premises Equipment).
- Memoria técnica.
- Incidentes.
- Análisis de tendencias.
- Plan de mejora de servicios.

La plataforma deberá cumplir con las siguientes funcionalidades:
Capacidad de dar seguimiento a los documentos e impedir que alguien pueda sobre-escribirlos, así como guardar una versión de cada documento en el que se hayan introducido cambios.

La información generada podrá ser consultada en el momento que el Instituto así lo considere necesario durante la vigencia del contrato, se deberá contar con la capacidad de realizar consultas históricas y respaldos de las muestras tomadas por cada sitio en medios magnéticos u ópticos.

La información de las muestras tomadas por sitio, reportes, documentos y demás productos que resulten de las actividades realizadas por el centro de monitoreo serán propiedad exclusiva del Instituto.

Al finalizar la vigencia del contrato, en un plazo no mayor a 2 meses, el proveedor deberá entregar en medios ópticos al Instituto toda la información que haya sido generada, así como eliminar la misma de sus equipos e instalaciones. El proveedor se compromete a guardar la confidencialidad de la información del Instituto generada en sus equipos durante la vigencia del contrato y de no divulgarla y hacer un mal uso de esta.

PARTIDA 2

El servicio objeto del presente contrato se prestará a partir del día siguiente de la notificación de la adjudicación y hasta el 31 de diciembre de 2020.

7.2. Servicio Administrado de Acceso a Internet

El proveedor deberá proporcionar el servicio de acceso a la red de Internet, para los nodos o inmuebles identificados en el Apéndice 2, sección en donde se define la capacidad requerida para cada uno de los nodos en cuestión. El servicio de acceso a Internet deberá proporcionarse conforme a los niveles de servicio establecidos en el presente documento.

El alcance de los servicios suministrados por el proveedor incluirá funcionalidades y servicios administrados de seguridad en cada uno de los 3 nodos listados en el Apéndice 2 "Inventario de Servicios de Acceso a Internet", mismos que con excepción del atributo de "Clean Pipes" (Capacidad de Mitigación de Ataques de Negación de Servicio) que debe estar integrado a cualquier Servicio de Acceso a Internet en los 3 nodos, serán cotizados de manera desagregada al servicio administrado de acceso a Internet (medio y acceso), tal y como se observa en el Catálogo de Servicios de este Anexo Técnico y en la Sección I "Precios Unitarios". Estas funcionalidades y servicios administrados de seguridad se describen más adelante en este anexo técnico.

Se deberá complementar la mitigación en la nube con la protección anti-DDoS en sitio para los portales web descritos en el anexo, incluyendo todos los elementos para la protección Web de los portales descritos en el anexo.

Debido a la importancia y criticidad de los Servicios Administrados de Acceso a Internet, éste deberá tener las siguientes características mínimas:

- Para tráfico hacia o desde el Instituto y con destino a una red o servicio dentro del Territorio Nacional se privilegiará el intercambio de tráfico en el IXP o por medio de acuerdos (peering) entre operadores nacionales a fin de que el tráfico generado en México permanezca en el territorio nacional.
- El proveedor deberá contar con acuerdos de interconexión globales (públicos y privados), los cuales faciliten el acceso a las aplicaciones y servicios digitales del IMSS
- El proveedor deberá ofrecer la mejor ruta y balanceo de carga inteligente basado en la utilización del enlace para mejorar el rendimiento y disponibilidad de las aplicaciones o servicios digitales que el IMSS considere críticos

El servicio a Internet deberá contar con un enlace alterno, que presente diversidad de acceso y de ruta en su red dorsal, así como la infraestructura necesaria para realizar la transferencia en caso de falla al enlace redundante desde el enlace activo (descritos en el Apéndice 2), permitiendo el acceso a las aplicaciones o servicios digitales del IMSS sin realizar cambio en el direccionamiento IP. Este enlace alterno deberá ser de infraestructura propiedad del proveedor.

Ambos enlaces de acceso a Internet (primario y alterno) deberán formar parte del backbone del proveedor de la partida 2, y estos enlaces deberán estar conectados hacia dos puntos diferentes del backbone de Internet del proveedor.

El IMSS cuenta actualmente con un segmento homologado de direcciones IP, por lo que es importante mencionar que los servicios que se tienen hoy en día están montados en el segmento antes mencionado. Inicialmente, el proveedor deberá proporcionar un bloque de 256 direcciones IP homologadas para el IMSS.

Este requerimiento, deberá permitir, cuando así sea solicitado por el IMSS, el incremento en bloques de 256 direcciones de IP homologadas sin generar costos adicionales.

El servicio de acceso a Internet deberá ser ofertado en un esquema en demanda, partiendo de un "piso" mínimo y con un "techo" máximo al cual se puede acceder con sucesivas ampliaciones con incrementales fijos y a precio unitario definido de acuerdo con el Catálogo de Servicios de esta contratación. El servicio será facturado y pagado por el IMSS con las características especificadas más adelante y de acuerdo con los rubros de servicio definidos en la Sección I "Precios Unitarios".

7.2.1. Requisitos Generales

El proveedor deberá proporcionar al IMSS el acceso a Internet cumpliendo los siguientes requerimientos, algunos de ellos ya introducidos en la sección anterior:

- El posible proveedor deberá demostrar, como parte de su Propuesta Técnica, que cuenta con enlaces de al menos un equivalente de 5 Gbps hacia el backbone de Internet y estas conexiones deberán estar en diferentes POP's, los cuales deben ser parte integral de la red del posible proveedor y no de un tercero.
- El posible proveedor deberá contar con acuerdos de interconexión globales (públicos y privados), los cuales deberán facilitar el acceso a las aplicaciones y servicios digitales del IMSS. Además de esto, el posible proveedor deberá de manifestar por escrito, como parte de su Propuesta Técnica, que cuenta con "Acuerdos de Intercambio" en el punto de intercambio de tráfico de Internet con por lo menos tres proveedores nacionales (y mencionar en el documento cuáles son estos proveedores)
- El posible proveedor deberá integrar, como parte de su Propuesta Técnica, copia de documentación en la que comprueben los "Acuerdos de Intercambio con por lo menos tres proveedores nacionales.
- El posible proveedor deberá integrar, como parte de su Propuesta Técnica, un diagrama genérico de su red de Internet. En el diagrama se deberán indicar las conexiones que se tienen hacia el punto de intercambio de tráfico de Internet, así como su capacidad.
- El posible proveedor deberá especificar, como parte de su Propuesta Técnica, que el medio para la entrega del servicio y la última milla serán con fibra óptica y deberá adjuntar un mapa del trayecto de la fibra desde el IMSS hasta el nodo del proveedor del acceso a Internet.
- El posible proveedor deberá ofertar, dentro de sus Propuestas Técnica y Económica, un acceso a Internet mediante enlaces de acceso en demanda con su respectiva redundancia, con la posibilidad de manejar anchos de banda mayores a 1 Gbps, usando una red de servicio metro ethernet para el acceso punto a punto, el cual deberá ser exclusivo para el IMSS, y no deberá ser multiplexado con otros servicios, teniendo como puntas de enlace para los enlaces activos y pasivos, Centros de Datos que prestan servicios al IMSS, de acuerdo a lo especificado en el Apéndice 2

Deberá proporcionar un direccionamiento completo clase C portable para el IMSS, soportando el protocolo BGP4 (Border Gateway Protocol).

7.2.1.1. Acceso a Internet Bajo Demanda

Las ubicaciones de los servicios de acceso a internet se detallan en el apéndice 2 del presente documento.

El Servicio Administrado de Acceso a Internet, como se ha mencionado, forma parte de la partida 2 de este ejercicio de contratación. El servicio en cuestión será facturado en demanda de acuerdo con el ancho de banda solicitado por el Instituto bajo el siguiente procedimiento de cálculo:

- El proveedor deberá cobrar el ancho de banda base, más los incrementales (de 10 MB) que apliquen. En caso de que los incrementales hayan sido solicitados durante el transcurso del mes, los incrementales se cobrarán de manera proporcional a los días devengados del mes, considerando meses de 30 días.
- El Proveedor deberá realizar el monitoreo diario del uso del circuito con poleos cada 5 minutos, tanto del tráfico de entrada como el de salida, para un total de 288 muestras de tráfico de entrada y otras 288 muestras de tráfico de salida.
- Se deberán ordenar las 288 muestras de entrada de manera decreciente, al igual se deberán de ordenar las 288 muestras de salida de manera decreciente.
- Se eliminará el 5% de las muestras mayores de entrada y el 5% de las muestras mayores de salida.
- Después de eliminar el 5% de ambas muestras (entrada y salida) se tomará la muestra mayor como muestra representativa del consumo del ancho de banda (Mbps) de dicho día.

- El mismo procedimiento se deberá realizar diariamente
- El servicio en cuestión será facturado en demanda de acuerdo al ancho de banda solicitado por el instituto bajo el siguiente procedimiento de cálculo: El proveedor deberá cobrar el ancho de banda base, más los incrementales (de 10 MB) que apliquen. En caso de que los incrementales hayan sido solicitados durante el trascurso del mes, los incrementales se cobrarán de manera proporcional a los días devengados del mes, considerando meses de 30 días.
- El cobro total se compondrá de la suma de las 30 lecturas diarias, con base mensual, con un consumo mínimo y un costo por cada 10 Mbps adicionales de acuerdo con la siguiente tabla:

Nodo de Internet	Inmueble	Piso (consumo mínimo garantizado)	Techo (consumo máximo)	Redundancia	Requerimientos Especiales	Usuarios o Consumidores aproximados (cifra referencial)
Nube IMSS Digital	Centro de Datos donde se aloja la "Nube IMSS Digital"	310 Mbps	1 Gbps	SI	Direcciones IP homologadas (no portables) que se requieran	Al menos 120,000 usuarios del IMSS
CeNaTi Nuevo León	CeNaTi Monterrey	155 Mbps	1 Gbps	SI	256 direcciones IP homologadas (no portables)	Al menos 256 servidores
CeNaTi México D.F.	CeNaTi México D.F.	32 Mbps	155 Mbps	SI	Direcciones IP homologadas (no portables) que se requieran	Al menos 20,000 usuarios del IMSS

El dominio que el proveedor manejará dentro de la solución es el asignado al IMSS (imss.gob.mx) con un DNS activo en Internet administrado por el proveedor.

El proveedor deberá garantizar una disponibilidad mínima del servicio del 99.98% de cada par de enlaces (dado que los 3 nodos son redundantes) de manera mensual en su backbone de conexión a Internet, así como los enlaces de última milla.

Gestión de Fallas especializada 7x24x365 con la certificación ISO 9002 o ISO 9001:2000 o ISO 20000 en cualquiera de sus versiones para brindar el máximo servicio (Centro de Atención de Fallas del Proveedor)

Deberá contar y proporcionar acceso a las personas que designe el IMSS a las siguientes aplicaciones en línea y que operen en tiempo real para verificar y garantizar el desempeño de la red:

- Estadísticas gráficas de tráfico, utilización del circuito de Entrada/Salida (IN/ OUT)
- El proveedor deberá incluir el cableado hasta el equipo de comunicaciones del IMSS a través de puertos Gigabit Ethernet en fibra óptica y donde se necesite a 10/100/1000 Mbps, el cual será su responsabilidad durante la duración del servicio así como el switch de acceso que forme parte del servicio propuesto. El punto físico de demarcación del servicio será el puerto físico del equipo de comunicaciones del IMSS en los nodos especificados. Se deberán brindar 2 puertos de 1GE Óptico (multimodo) y 2 puertos de cobre 10/100/1000.

En la propuesta técnica, el Posible proveedor debe mencionar que entregará el servicio en fibra óptica, nombre de la empresa que proporcionará la última milla y un mapa del trayecto de la fibra desde los nodos del IMSS especificados en el Apéndice 2, hasta el nodo del proveedor del acceso a Internet.

7.2.1.2. Arquitectura del Servicio

El servicio de acceso a Internet será utilizado por dos tipos de usuarios, el interno del IMSS (funcionario) y el externo (ciudadano). El externo normalmente utilizará este servicio al ingresar a las paginas institucionales del IMSS, para la realización de algún trámite o consulta institucional; el usuario interno del IMSS necesita de este servicio para la transacción de información con otras instituciones, ya sea gubernamentales, de salud o bancarias, o para comunicarse con el derechohabiente para la realización de un trámite con la institución, por mencionar solo algunas de las funciones.

El proveedor deberá ofrecer al IMSS un servicio de Internet de las siguientes características, para cada uno de los enlaces activos definidos en el Apéndice 2:

- Internet bajo demanda con posibilidad de transferencia (velocidad) "piso" de 310, 155 y 32 Mbps, respectivamente, de acuerdo con la tabla anterior especificada en la sección "Acceso a Internet Bajo Demanda"
- Alta disponibilidad del servicio con posibilidad de uso de protocolo HSRP en equipo CPE
- Servicio de mitigación de Ataques de Denegación de Servicio Distribuido (DDoS Clean Pipes, como es conocido en idioma inglés)
- Servicio de Balanceo vía BGP

El posible proveedor de servicio deberá ofrecer conectividad a Internet utilizando infraestructura de red Metro Ethernet, entregando una conexión punto-a-punto o punto extendida a lo largo de la red posible proveedor hacia los puntos de demarcación. Se definirá una VLAN para el servicio de Internet.

Punto de Demarcación:

Los Servicios Administrados de Acceso a Internet que se entregarán en los tres Nodos Centrales de la Institución, deberán considerar que éstos cuentan con distintos niveles y tipos de Infraestructura frontera, a la que habría que conectar la infraestructura propia del proveedor para poder ofrecer los servicios solicitados.

Los posibles proveedores deberán considerar, como parte de sus propuestas y económicas, toda la infraestructura, licenciamiento, cableado, servicios de soporte técnico, garantías extendidas, mantenimiento, operación, además de toda la infraestructura habilitadora y red de telecomunicaciones requeridas, y que permitan brindar el Servicio de Internet con las siguientes características:

- Servicio de Internet dedicado, entregado a través de infraestructura propiedad del posible proveedor en enlaces Ethernet con interfaces de 1 Gbps, de acuerdo a la infraestructura de frontera exhibida para cada nodo en la sección "Perfil para Centro de Datos". Los servicios de conectividad solicitados deberán contar con mecanismos de redundancia en todos los elementos activos y pasivos usados para transportar y brindar conectividad a los enlaces solicitados. Para dar cabal cumplimiento a la solicitud de redundancia para cada uno de los nodos solicitados, los posibles proveedores deberán incluir en sus propuestas técnicas que cada nodo deberá recibir el servicio con las siguientes características de conectividad:
- Enlaces redundantes en configuración activo-activo. El tráfico de cada Nodo deberá estar balanceado entre los dos enlaces en configuración activo-activo, y la medición de ancho de banda del nodo será el resultante de la suma del tráfico en ambos. Los enlaces redundantes deberán estar configurados para permitir el transporte del ancho de banda solicitado en el nodo, a pesar de que uno de los enlaces esté fuera de servicio. Es importante aclarar que el ancho de banda solicitado para cada nodo se compone de la suma resultante del "piso" de ancho de banda solicitado inicialmente, más todos los incrementos de ancho de banda consumidos en dicho momento para dicho nodo, a través del "Servicio de Incremento de Ancho de Banda para Internet" de este Anexo Técnico.
- Equipos de transporte de "última milla" en las terminales de los sitios del IMSS en cada Centro de

Datos, donde la infraestructura sea completamente redundante en todos sus componentes activos, tal como: Fuentes de Poder redundantes, tarjetas de enlaces de fibra, tarjetas controladoras y/o procesadoras, etc.

- Equipos de Ruteo redundante. En los Nodos donde se requiere que el proveedor entregue el Servicio de Internet, a través de ruteadores, éstos deberán ser redundantes y el servicio deberá incluir al menos dos ruteadores en cada nodo central. Los enlaces redundantes, deberán interconectarse uno a cada ruteador. Adicionalmente, la configuración de los equipos deberá considerar la existencia del ruteador redundante, de tal forma que en el evento de la caída de uno de los ruteadores, o los enlaces de Internet mismo, todas las funciones y tráfico del nodo sean completamente absorbidos por el equipo sobreviviente al evento. Esta transición de redundancia deberá suceder de manera automática e inmediata ante la caída, y deberá reestablecerse a su condición de operación normal, una vez que el ruteador y enlace fallido se reestablezca. La configuración de los equipos, enlaces y protocolos de ruteo deberá hacerse de tal forma que permita cumplir y/o exceder los Niveles de Servicio solicitados por el IMSS.
  La redundancia que se solicita se refiere a un esquema de N+1 en toda la solución del nodo nube IMSS digital.
  Deberá brindar 2 puertos de 1GE Óptico (multimodo) y 2 puertos de cobre 10/100/1000.
- Enlaces de red Ethernet entre los equipos de frontera detallados en la sección "Perfil para Centro de Datos" y los equipos de ruteo del proveedor, y/o equipo de transporte de última milla aquí descritos. Los enlaces Ethernet deberán ofrecerse en fibra óptica, y deberán considerar el tipo de fibra óptica y conectores específicos de cada nodo, debiendo ser dichos enlaces infraestructura propiedad del posible proveedor.

Es importante aclarar que los posibles proveedores deberán incluir todos estos requerimientos como parte de los Servicios Administrados de Acceso a Internet, y que el IMSS no incurrirá en ningún costo adicional al detallado en el Catálogo de Servicios y en la Sección I: Precios Unitarios.

Ancho de Banda:
El Ancho de Banda del servicio deberá ser configurable en demanda desde un piso de 310, 155 y 32 Mbps, de acuerdo con la tabla especificada en la sección "Acceso a Internet Bajo Demanda" y con incrementos (paquetes de cobro por consumo mensual) de 10 Mbps, hasta llegar a un máximo de 1 Gbps.

Tráfico:
El tráfico de LAN transportado en la red Metro Ethernet deberá recibir tratamiento de capa 3 hacia los equipos que proporcionan la salida a Internet del proveedor de servicio.

Los anuncios de las redes del IMSS serán realizados por el (los) equipo(s) del proveedor, respetando todas las políticas de anuncios que tienen el resto de los equipos de la red de Internet.

Los servicios Ethernet ofrecidos deberán de poder ser limitados en su ancho de banda dentro de las capacidades físicas de las interfaces ópticas o eléctricas en las que se entreguen, de tal forma que se puedan tener techos máximos de consumo ajustables en los intervalos solicitados por el IMSS.

Multi-homming:
El IMSS requiere un servicio de Internet que pueda ser parte de una arquitectura multi-homming donde se tenga una convivencia del servicio con dos o más proveedores de servicio de Internet (ISP), bajo un sistema que permita la manipulación de tráfico y distribución de cargas por medio del protocolo de enrutamiento BGP4 (Border Gateway Protocol). Por lo anterior, el posible proveedor deberá considerar la posibilidad de enlazar el

CPE que provea con su solución, con el CPE del proveedor de Internet ISP alterno vía el protocolo I-BGP-4 para el manejo adecuado de todos los criterios y métricas disponibles y posibles del mismo protocolo para configurar en este tipo de ambientes.

Servicio de Balanceo vía BGP:
El Proveedor deberá integrar un sistema completo y automatizado de balanceo de carga vía BGP, mismo que deberá interactuar con los CPEs provistos por el mismo proveedor, así como con los provistos por el ISP alterno de Internet.

Disponibilidad:
El IMSS requiere de una disponibilidad, en ambos servicios, del 99.98% en su backbone de conexión hacia Internet. Para el caso del enlace de última milla, se deberá garantizar un valor de disponibilidad de 99.98%.

Monitoreo y Reportes:
El proveedor deberá proporcionar una herramienta, basada en Web, que permita obtener reportes de desempeño del servicio hacia Internet.

Los formatos de los reportes y la frecuencia de entrega se elaborarán de común acuerdo entre el IMSS y el proveedor. Dichos reportes podrán ser exportados a formatos tales como HTML, PDF, ASCII y Excel.

7.2.1.3. **Componentes Habilitadores para Internet**
Para el caso de nuevos requerimientos, a continuación, se enlistan los requisitos y funcionalidades mínimas que deberán cumplir los equipo CPE para el Servicio Administrado de Acceso a Internet, de acuerdo con la arquitectura previamente definida:

- El proveedor deberá proporcionar equipos CPE's (Customer Premise Equipment), para recibir en los sitios especificados en el Apéndice 2, los enlaces de comunicaciones del servicio de Internet.
- El proveedor deberá proporcionar la infraestructura y red de telecomunicaciones y enlaces para Internet.
- El proveedor deberá proveer al IMSS acceso de tipo "lectura" a la configuración de cualquier equipo CPE que incluya con la solución y, a su vez, deberá homologar las configuraciones de sus equipos CPE con los del ISP alterno descrito en la arquitectura del servicio. El IMSS podrá en todo momento revisar las configuraciones de los equipos y participar en el establecimiento de los Acuerdos de Nivel de Operación (OLAs) entre los distintos ISPs.
- Con el fin de contar con un servicio homogéneo a nivel nacional, los equipos CPE's deberán cumplir con el modelo y las características mínimas descritas más adelante.
- Los posibles proveedores deberán incluir en su Propuesta Técnica un listado de los equipos que integran su solución, junto con diagramas con el diseño propuesto, en los que se identifique en forma clara y detallada el apego a la arquitectura y a la topología aquí descrita.

- El proveedor será responsable de:
  - La continuidad del servicio en los nodos o inmuebles especificados por el IMSS en el Apéndice 2
  - La configuración lógica y física de los equipos CPE's
  - La configuración del equipamiento sitio por sitio, con base en el diseño basado en la arquitectura descrita en este documento, y en la ingeniería del proveedor
  - El mantenimiento correctivo del equipo
  - El respaldo y reposición de equipo en caso de falla, incorporando un equipo de iguales o mayores capacidades

- Los traslados y horas-ingeniero para las actividades mencionadas anteriormente
- La creación de los perfiles de la red del cliente en las plataformas de administración
- Las pruebas de turn-up de la red punta a punta
- La realización de altas, bajas, cambios y movimientos lógicos

Descripción de alto nivel de los componentes habilitadores:

- CPE de Internet
  - Deberá contar con la suficiente capacidad en hardware para soportar el procesamiento de todo el tráfico que el IMSS demande en su servicio de Internet, conformado por un par de equipos switch/router capa 3 del modelo de la OSI, con el máximo de memoria y procesador de alto desempeño.
  - Deberán tener las posibilidades de recibir la tabla completa de rutas del Internet, enrutar usando protocolos como OSPF, BGP, Estático.
  - Deberá proveer capacidades de conmutación a nivel 2 y 3 de la OSI de alto desempeño, que sirva de distribución del servicio de Internet hacia el interior de la infraestructura del IMSS. Aquí se podrán aplicar, de manera enunciativa más no limitativa, el manejo óptimo de políticas de enrutamiento internas y externas, listas de acceso, QoS, entre otros.
  - Deberá contar con conexiones 10/100/1000 y conexiones 1 GE óptico.

7.2.1.4. **Servicios de Seguridad para el Nodo "Nube IMSS Digital"**

En virtud de que el IMSS se encuentra consolidando la plataforma que le permitirá el alojamiento de servicios digitales de nueva generación, en el Centro de Datos que le presta servicios bajo el concepto "Nube IMSS Digital", la mayor parte de las funcionalidades de seguridad en sitio que serán aplicadas al tráfico de Internet, serán provistas por el IMSS dentro de esta plataforma. Por esta razón, el proveedor únicamente deberá entregar el tráfico de Internet atendiendo al punto de demarcación descrito en la "Arquitectura del Servicio" y entregando dicho tráfico a la plataforma mencionada, sin perder de vista los atributos de "Clean Pipes" (Capacidad de Mitigación de Ataques de Negación de Servicio) y los mencionados previamente, para darle al IMSS garantía de limpieza de los datos en dichos aspectos. **Es por ello que únicamente existe un elemento en el Catálogo de Servicios, denominado "Servicios Administrados de Acceso a Internet para Nodo "Nube IMSS Digital", que cubre la totalidad de servicios requeridos en este nodo, de manera mensual.**

7.2.1.5. **Servicios de Seguridad para el Nodo "Monterrey"**

Para el caso del Servicio Administrado de Acceso a Internet entregado en el Nodo CeNaTi Monterrey, listado con mayores detalles respecto de su ubicación en el Apéndice 2, el Proveedor deberá proporcionar servicios de seguridad asociados con el tráfico de Internet a ser consumido por el IMSS.

El proveedor considerará, para este nodo, los costos de estos servicios de manera desagregada (separada) del Precio Unitario Mensual correspondiente a este acceso a Internet dentro del Catálogo de Servicios, con excepción del servicio de Clean Pipes (Capacidad de Mitigación de Ataques de Negación de Servicio), mismo que se considera integrado al Precio Unitario Mensual del Acceso a Internet. Toda la infraestructura de hardware y software que el Proveedor incorpore para cumplir con estos requisitos deberá ser nueva y de uso exclusivo para el IMSS, no usada ni reconstruida.

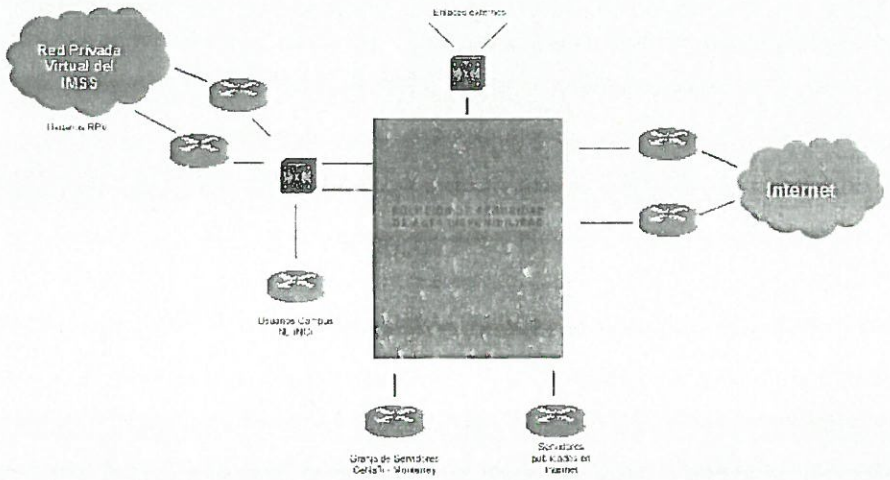
De manera enunciativa más no limitativa, los requerimientos técnicos del IMSS en este sentido para con el proveedor son:

- Administrar la solución de seguridad propuesta para cumplir los requerimientos funcionales descritos. Adicionalmente, deberá proporcionar en las instalaciones del IMSS (en la ciudad de México) un sistema

de supervisión para todos los elementos de la solución, similar a la que encuentre operando como parte de la solución del proveedor, para la comprobación de las funcionalidades requeridas por el IMSS y que cuente con la capacidad de al menos 10 usuarios concurrentes.

- Poner en operación la solución localizada de seguridad basándose en las políticas operativas existentes en el ambiente de seguridad actual, mismas que serán compartidas por el Administrador del Contrato al proveedor durante mesas de trabajo. Se realizará un análisis de vulnerabilidades sobre la infraestructura de red en el CeNaTi - Monterrey y sobre la propia solución de seguridad, a fin de que se identifiquen los aspectos de vulnerabilidad en la seguridad de la infraestructura del IMSS
- Proporcionar un esquema de replicación inmediata de las modificaciones en las políticas de los diferentes elementos y dispositivos que conformen la solución de seguridad específica para el Nodo CeNaTi Monterrey.

El proveedor deberá incluir el hardware y/o software necesarios para proporcionar al menos las siguientes funcionalidades tomando el diagrama como referencia:



- Solución en Alta Disponibilidad de Prevención de intrusos (IPS), que apoye a asegurar los servicios publicados por el IMSS y red interna Institucional y que soporte al menos 120,000 usuarios concurrentes)
- Solución en Alta Disponibilidad de Firewall, que soporte al menos 120,000 usuarios concurrentes
- Solución en Alta Disponibilidad de análisis de flujo con capacidad de detección de anomalías en tráfico
- Solución de Mitigación de Ataque de Negación de Servicios

El canal de comunicación y capacidad de procesamiento de cada elemento en la solución de seguridad debe estar dimensionado con una política de al menos cuatro veces mayor al respectivo enlace a Internet, dependiendo del origen/destino de la información.

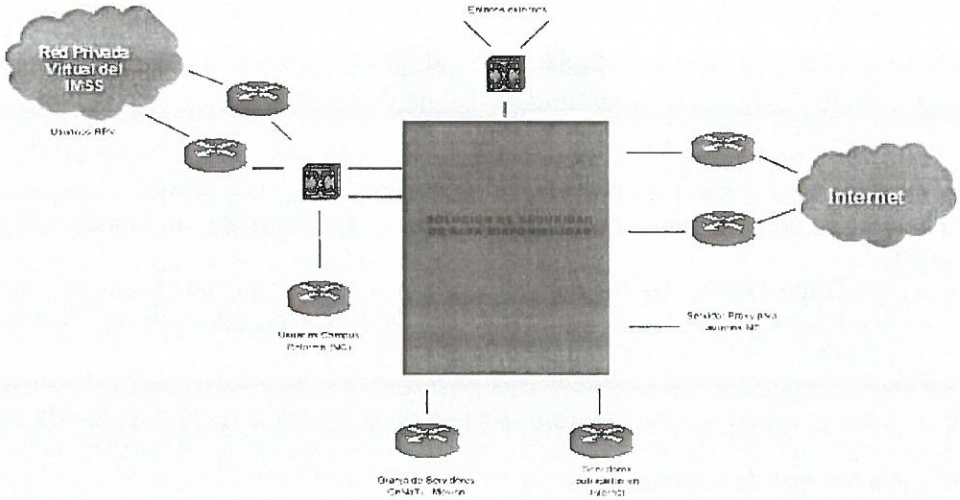
7.2.1.6. **Servicios de Seguridad para el Nodo "D.F."**

Para el caso del Servicio Administrado de Acceso a Internet entregado en el Nodo CeNaTi D.F., listado con mayores detalles respecto de su ubicación en el Apéndice 2, el proveedor deberá proporcionar servicios de seguridad asociados con el tráfico de Internet a ser consumido por el IMSS.

El proveedor deberá incluir, para este nodo, los costos de estos servicios de manera desagregada (separada) del Precio Unitario Mensual correspondiente a este acceso a Internet dentro del Catálogo de Servicios, con excepción del servicio de Clean Pipes (Capacidad de Mitigación de Ataques de Negación de Servicio), mismo que se considera integrado al Precio Unitario Mensual del Acceso a Internet. Toda la infraestructura de hardware y software que el proveedor incorpore para cumplir con estos requisitos deberá ser nueva y de uso exclusivo para el IMSS, no usada ni reconstruida.

De manera enunciativa más no limitativa, los requerimientos técnicos del IMSS en este sentido para con el proveedor son:

- Administrar la solución de seguridad propuesta para cumplir los requerimientos funcionales descritos. Adicionalmente, deberá proporcionar en las instalaciones del IMSS (en la ciudad de México) un sistema de supervisión para todos los elementos de la solución, similar a la que se encuentre operando como parte de la solución del Proveedor, para la comprobación de las funcionalidades requeridas por el IMSS y que cuente con la capacidad de al menos 10 usuarios concurrentes.
- Poner en operación la solución localizada de seguridad basándose en las políticas operativas existentes en el ambiente de seguridad actual, mismas que serán compartidas por el Administrador del Contrato al proveedor durante las mesas de trabajo. Se realizará un análisis de vulnerabilidades sobre la infraestructura global de red y sobre la propia solución de seguridad, a fin de que se identifiquen los aspectos de vulnerabilidad en la seguridad de la infraestructura del IMSS
- Proporcionar un esquema de replicación inmediata de las modificaciones en las políticas de los diferentes elementos y dispositivos que conformen la solución de seguridad específica para el Nodo CeNaTi D.F.
- El proveedor Incluirá el hardware y/o software necesario para proporcionar al menos las siguientes funcionalidades tomando el diagrama como referencia:



- Solución en Alta Disponibilidad de Prevención de intrusos (IPS) que apoye a asegurar los servicios publicados por el IMSS y red interna Institucional y que soporte al menos 20,000 usuarios concurrentes
- Solución en Alta Disponibilidad de Firewall que soporte al menos 20,000 usuarios concurrentes
- Solución en Alta Disponibilidad de análisis de flujo (con capacidad de detección de anomalías en tráfico)
- Solución de Mitigación de Ataque de Negación de Servicios
- Solución en Alta Disponibilidad de Control de Acceso a Páginas Web (dimensionado por lo menos para 20,000 usuarios)

El canal de comunicación y capacidad de procesamiento de cada elemento en la solución de seguridad debe estar dimensionado con una política de al menos cuatro veces mayor al respectivo enlace a Internet, dependiendo del origen/destino de la información.

7.2.1.7. Funcionalidades Detalladas de Seguridad

A continuación, se describen con mayor detalle, las funcionalidades mínimas requeridas para cada uno de los servicios de seguridad asociados a los diferentes accesos (nodos) de Internet, de manera que obren como referencia para una adecuada selección de componentes habilitadores que permitan su entrega y cumplimiento bajo el esquema seleccionado de Servicios Administrados.

Todos los Componentes Habilitadores propuestos por el posible proveedor y requeridos para otorgar las soluciones de seguridad específicas que se enlistaron para cada uno de los Nodos de Internet previamente definidos, deberán tener la capacidad de proveer las funcionalidades de seguridad solicitadas a continuación en cada servicio.

El posible proveedor deberá incluir en su propuesta un listado de los componentes habilitadores que integran cada uno de los servicios solicitados a continuación, indicando la marca, el modelo y las características de cada uno de ellos, demostrando de forma explícita de qué manera se atienden las funcionalidades mínimas solicitadas. Además, deberán incluir diagramas con el diseño de alto nivel propuesto, en donde se identifique en forma clara y detallada la solución solicitada en cada uno de los servicios.

Con el fin de contar con un servicio homogéneo, todos los componentes habilitadores que sean propuestos por el posible proveedor para la integración de cada uno de los servicios específicos de seguridad deberán ser del mismo fabricante. Lo anteriormente dicho no implica que todos los componentes habilitadores de todos los servicios de seguridad solicitados por el IMSS para los Nodos de Internet sean del mismo fabricante, sino que deberá mantenerse esta condición para los componentes que integran las soluciones individuales (por ejemplo, la solución de firewall versus la de filtrado pueden ser de fabricantes distintos, pero todos los componentes habilitadores de cada una de ellas sí deberán de ser del mismo fabricante).

El posible proveedor deberá observar, con independencia de los componentes habilitadores de seguridad elegidos, otorgar siempre al IMSS el cumplimiento de los Niveles de Servicio específicos, descritos en la sección "Requerimientos de Nivel de Servicio".

Adicionalmente, es requisito indispensable que el proveedor cuente con el soporte, por parte de expertos del fabricante de cada una de las soluciones ofertadas, manteniendo así posibilidades de escalación directa con los mismos y sus respectivas áreas de desarrollo y soporte. El proveedor llevará a cabo, como parte del servicio asociado a cada una de las soluciones a detallar a continuación, de manera enunciativa más no limitativa, lo siguiente:

1. Provisión de los componentes habilitadores e instalación de los mismos en los nodos de acceso a Internet especificados en los Apéndices de esta contratación.
2. Interconexión de estos componentes habilitadores con los equipos de comunicaciones del Centro de Datos en cuestión.
   Para el "Nodo IMSS Digital", el Instituto solo brindará la coubicacion (energía eléctrica protegida y regulada, unidades de rack, puertos de Lan Switch y cableado estructurado).
   Por lo que el posible proveedor, deberá indicar al Instituto lo correspondiente a la cantidad y tipo de puertos, contactos eléctricos con el amperaje y voltaje requerido, espacios en unidades de Rack y la infraestructura auxiliar que solicite.

3. Para los nodos de DF y Monterrey, el Instituto solo brindará espacio físico y energía regulada, por lo que el posible proveedor deberá incluir en su proposición toda la infraestructura auxiliar que requiera
4. Configuración del equipamiento con base a las premisas de alto nivel expresadas en estos Anexos Técnicos.
5. Mantenimiento correctivo
6. Respaldo y reposición de equipo en caso de falla, respetando los Niveles de Servicio establecidos
7. Traslados a los sitios, considerando las horas de ingenieros para dar cumplimiento a los tiempos y condiciones explicados en este Anexo Técnico
8. Creación de los perfiles de la red del IMSS en las plataformas de administración correspondientes
9. Pruebas de turn-up de la red punta a punta, indispensables previo a la liberación y aceptación de cada una de las soluciones por parte del Administrador del Contrato en el IMSS
10. Altas, bajas y cambios.
11. Administración, gestión y operación.
12. Provisión de infraestructura auxiliar necesaria para la correcta operación de los servicios en los Centros de Datos mencionados, pudiendo ser ésta (de manera enunciativa mas no limitativa): racks, UPS, tierra física, cableado estructurado, entre otros.

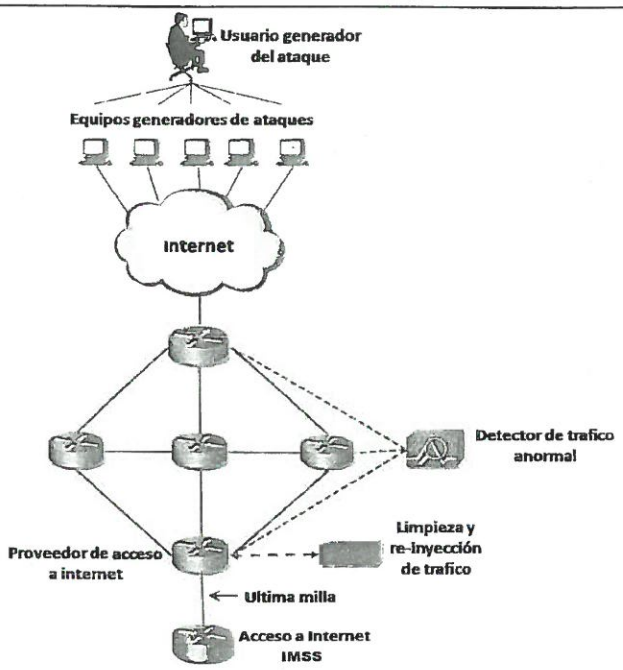
7.2.1.8. **Solución o Capacidad de Mitigación de Ataque de Negación de Servicios (Clean Pipes)**
Se requiere que en la infraestructura del proveedor se incluya un mecanismo para determinar en forma automática el comportamiento anómalo del servicio y tener la capacidad de alertar al IMSS para mitigar cualquier actividad maliciosa que se presente, como ataques de negación de servicio o negación distribuida de servicio (DoS/DDoS, por sus siglas en inglés) generado por medio de la actividad de gusanos o de ataques de tipo botnets.

Como se mencionó anteriormente, esta solución o capacidad SÍ se encuentra integrada al precio unitario de los Servicios Administrados de Acceso a Internet de cada nodo, y no a los Servicios Administrados de Seguridad de cada nodo.

Por tanto, el servicio deberá integrar un sistema de gestión de amenazas que realice una inspección profunda de paquetes, que permita al proveedor del servicio reducir de manera rápida e inteligente las amenazas a la seguridad y contra cualquier situación desconocida que trate de agotar alguno de los recursos de los sistemas de comunicaciones, tales como el ancho de banda, saturación de búferes, saturación de discos duros o los recursos informáticos de la red.

A continuación, se mencionan algunas de las amenazas que, como mínimo, el sistema de mitigación de ataques de proveedor que deberá eliminar:

- Ping de la muerte
- Ataque por inundación SYN
- Fragmentación de paquetes y reensamblaje
- Broadcast de correo electrónico
- Saturadores de CPU
- Scripts generadores de tráfico
- Generadores de caracteres
- Ataques fuera de banda (WinNuke)
- Ataque Smurf (generador de gran cantidad de paquetes ICMP)



La funcionalidad de protección ofrecida tendrá las siguientes características:

Monitoreo y Detección

- Ingeniería de tráfico inteligente: Visibilidad escalable y análisis del tráfico con tecnología de "Flujo de Red"
- El análisis del tráfico con la tecnología de "Flujo de Red" deberá de realizarse en los enrutadores del Proveedor, y de manera indispensable, en el equipo que provee el servicio de Internet a los enlaces del IMSS, en los enrutadores conectados a Internet y en los enrutadores conectados a Internet de sus demás clientes.
- Tanto la limpieza del tráfico como la re-inyección de éste, deberán realizarse lo más cercano posible al equipo CPE que entrega el servicio de Internet por parte del proveedor.
- Deberá garantizar el paso transaccional legítimo.
- Deberá mantener una operación libre de problemas para los recursos críticos del negocio.
- Detección del tráfico basado en el lenguaje TCPDUMP (con información definida en las capas 3 y 4); será posible utilizar el Netflow para la revisión de TCP DUMP siempre y cuando cumpla con lo solicitado en el numeral de referencia y los niveles de servicios.
- El sistema deberá tener la capacidad de advertir anticipadamente algún posible ataque, analizando tendencias de tráfico malicioso en tiempo real.
- El proveedor deberá de tener capacidad de monitoreo en tiempo real de los circuitos dedicados que entregan la conectividad a Internet para detectar el comportamiento anormal del tráfico que pueda estar dirigido a atacar las interfaces de los enrutadores implicados en el enlace.
- El proveedor deberá de tener la capacidad de monitoreo en tiempo real de la subred (pública) que conectan los enlaces, para que permita la detección de tráfico anormal que pueda significar un ataque dirigida a ella.
- El proveedor deberá de tener la capacidad de monitoreo en tiempo real de los activos informáticos conectados en la subred pública para detectar tráfico anormal que pueda significar un ataque dirigido a éstos.

- Detección de ataques basado en la línea de base contra los recursos definidos, con opciones configurables por recursos que permitan filtrar la sensibilidad de la anomalía y disparar una alarma, en paquetes por segundo y Mbps.
- El proveedor deberá monitorear las siguientes variables en tiempo real para garantizar los Niveles de Servicio:
  - Para el protocolo IP:
    - ICMP
    - Paquetes IP fragmentados
    - Paquetes IP NULL
    - Paquetes IP con direcciones privadas
  - Para el protocolo TCP:
    - Segmentos TCP NULL
    - Segmentos TCP RST
    - Segmentos SYN
    - Tráfico total
- La funcionalidad propuesta por el proveedor de servicio deberá como mínimo detectar los siguientes tipos de ataques DoS/DDoS sobre las interfaces, subredes y activos informáticos protegidos del IMSS:
  - ACK Flood
  - SYN Flood
  - Hogging CPU
  - Chargen (Character generator)
  - FIN Flood
  - ToS Flood
  - DNS Malformed
  - HTTP Flood
  - ICMP Flood
  - UDP Flood
  - Non- UDP/TCP/ICMP Protocol Flood
  - PPS Flood Attack
  - Zombie attack
  - Land Attack

- La solución propuesta del proveedor deberá de permitir la personalización de los niveles de alarma o umbrales que sirvan para la detección de ataques, a una granularidad por objeto monitoreado.
- La solución propuesta por el proveedor de servicio deberá monitorear actividad sospechosa que pueda significar algún ataque de gusanos o "Worms" o virus.
- La solución propuesta por el proveedor de servicio deberá monitorear actividad "Dark IP"
- Detección de anomalías DDoS y amenazas de día cero antes de que impacten en los servicios.
- Por el detalle del monitoreo y detección, la solución propuesta por el proveedor de servicio deberá de estar basada en el uso del "Flujo de Red" en la red proveedor de servicio, más no en la red del IMSS, evitando la instalación de equipo para este propósito en las facilidades de dicha entidad.
- Detección de zombis (con selecciones de umbrales en Mbps y pps desde el portal Web del cliente) para clasificar una IP como zombis y con la opción de conocer una lista de zombis activos detectados.

Complementar la mitigación en la nube con la protección anti-DDoS en sitio para los portales web descritos en el anexo, incluir todos los elementos.

Mitigación:

- En el caso de que se tenga confirmación de un ataque detectado sobre el enlace, subred o activo del IMSS, el proveedor deberá ser capaz de ejecutar una mitigación apropiada para el tipo de ataque DoS/DDoS en progreso.
- Mitigación de DDoS y amenazas de día cero antes de que impacten en los servicios del IMSS
- Una vez que se ha detectado esta condición anómala, el tráfico deberá ser filtrado y descartado todo el tráfico dañino, dejando pasar solo el tráfico legítimo hacia las redes del IMSS para ser entregado a su destino final; durante todo este proceso los servicios publicados en Internet deben permanecer siempre disponibles.
- El proveedor deberá llevar a cabo la mitigación lo más alejado posible de la red del IMSS, ejecutándola en los puntos de interconexión de su red con otros proveedores de servicios ISP, para el caso de un ataque que provenga desde afuera de la red del proveedor de servicio, o bien se deberá ejecutar en los enrutadores de acceso a Internet en el caso de un ataque originado desde la misma red del proveedor de servicio, evitando en todo momento hacerlo en los enlaces, subredes o activos del IMSS. Esto con el objetivo de mantener los recursos del IMSS disponibles para el tráfico legal.
- El proveedor deberá comprobar al IMSS mediante documentación y diagramas topológicos de diseño, que la detección de flujos anómalos se realiza no solo en sus interconexiones principales de Internet, sino también a la infraestructura que provee el servicio de Internet al IMSS.
- El análisis del tráfico, la detección de anomalías y el proceso de mitigación de ataques de tipo DDoS se debe llevar a cabo en la infraestructura del proveedor del servicio, el objetivo es que el proceso de mitigación del tráfico de ataque se realice antes de que pueda llegar a las redes del IMSS.
- Durante la mitigación, el proveedor deberá de desviar el tráfico para limpiarlo, bloqueando o eliminando solo y únicamente el tráfico anómalo o ilegal, el tráfico normal o legal deberá de poder seguir usando los recursos del IMSS.
- Cuando el proveedor tenga confirmación de que el ataque ha terminado, el flujo de los datos deberá de seguir su curso normal hacia el IMSS
- Para los ataques detectados, se debe ofrecer la opción de generar recomendaciones de listas de acceso basadas en cada ataque.
- Se permitirá al proveedor seleccionar la mitigación a aplicarse.
- La solución debe permitirle al proveedor del servicio la inicialización de mitigaciones con:
  - Inyección de Blackhole de BGP
  - Filtros con listas de acceso (ACLs)
  - Dispositivos de mitigación que deben ofrecer una mitigación inteligente, filtrar tráfico malicioso mientras se permite el tráfico válido para alcanzar el elemento que está siendo atacado
- El proveedor deberá poder implantar tecnología para procesar el máximo de ancho de banda de Internet de los enlaces solicitados.
- Deberá permitir ancho de banda adicional para ser adicionado hasta la petición del cliente
- La mitigación debe ofrecer por lo menos las siguientes características:
  - Mitigación de específico SYN Flood
  - Mitigación del DNS (protocolo mal formado y basado en autenticación)
  - Mitigación con tasa límite por cliente de HTTP Get Flood y por objeto
  - Línea de base por recurso

Proceso de mitigación:

- Ante una alarma de tráfico anormal, el proveedor a través de su centro de monitoreo deberá contactar al personal designado por el IMSS para notificar del incidente y en su caso solicitar autorización para mitigar.
- El Proveedor deberá iniciar la mitigación de manera automática para el ataque DoS/DDoS "http flood"

cuando así se haya pactado con el IMSS para este tipo de incidentes.

- El proveedor deberá de establecer contacto con el IMSS mediante teléfono, teléfono móvil o correo electrónico.
- El proveedor deberá de tener que garantizar que este será un proceso operativo en un marco de 7x24 horas los 365 días del año.
- Cuando el ataque haya sido mitigado, el proveedor deberá de notificar al Administrador del Contrato en el IMSS usando los medios descritos anteriormente.
- Si el IMSS llega a detectar algún comportamiento anormal, podrá contactar al centro de atención del proveedor de servicio para verificar el estado de los recursos en términos de ataques de DoS/DDoS.
- El posible proveedor deberá integrar en su proposición un esquema detallado de esta solución indicando los elementos que la integran, así como la descripción de los procesos de análisis de información, detección de anomalías y mitigación de ataques.
- Esta solución se requiere en la infraestructura del Proveedor (servicio ubicado en su nube)

Reportes:

- El proveedor deberá facilitar al IMSS un portal Web para acceder a reportes vía Internet
- El portal Web deberá proporcionarle al IMSS toda la visibilidad de los ataques que están ocurriendo en su red.
- Se deberán ejecutar reportes en tiempo real y agendados que incluyan lo siguiente:
- Anomalías clasificadas por niveles de severidad (configurada por el IMSS)
- El Portal deberá de ser personalizable, donde las plantillas puedan ser creadas para ver recursos específicos, reportes, ataques, así como, inicializar especificas mitigaciones y contador de medidas para reducir el impacto de esos ataques, todo desde la misma página Web
- Por lo menos se debe proveer acceso a los últimos 3 meses de las alertas y las mitigaciones ocurridas
- El proveedor de servicio deberá mostrar en pantalla estos reportes en hipertexto y gráficos usando navegadores Internet Explorer, Chrome y Firefox, hasta las versiones más recientes de éstos
- Los reportes podrán ser descargados por el IMSS en formato XML, PDF, Excel.xml y CSV
- El IMSS y el Proveedor podrán enviar los reportes por correo electrónico desde el mismo portal hacia cuentas de correo de uso público, como cuentas internas del IMSS
- A través de la misma página Web deberá permitir la generación de plantillas de ataques conocidos
- Debe permitir al proveedor generar reportes de las mitigaciones que fueron ejecutadas anteriormente, con detalles de tráfico que pasó y tráfico que se descartó para cada uno de los medidores, accesibles al IMSS
- El Proveedor deberá de garantizar que los reportes como mínimo serán sobre:
    - Alertas "en proceso" y recientes, los cuales deben de mostrar:
        - Resumen de la alerta:
        - Identificación del evento
        - Relevancia
        - Impacto
        - Hora de inicio y fin
        - Dirección
        - Tipo
        - Recurso afectado
    - Caracterización del tráfico:
        - Fuentes y puertos
        - Destinos y puertos
        - TCP Flags
        - Protocolo

- Gráficas del ancho de banda consumido contra tiempo, en bits- por- segundo y paquetes- por- segundo

o Elemento de red afectado
- Relevancia
- Valor esperado
- Valor observado en bits por segundo
- Valor observado en paquetes por segundo
- Gráficas del ancho de banda consumido contra tiempo, en bits- por- segundo y paquetes- por- segundo

o Detalles del tráfico
- Direcciones IP y máscara
- Bytes
- Paquetes
- Bytes/paquete
- Bits por segundo
- Paquetes por segundo
- % en bits por segundo
- Rango de puertos
- Protocolo

o Reporte sobre "Toptalkers" internos
- Tabla que resuma el host y el peakrate
- Gráfica de Toptalkers versus ancho de banda en bits por segundo y paquetes por segundo

o Reporte sobre "Toptalkers" externos
- Tabla que resuma el host y el peakrate
- Gráfica de Toptalkers versus ancho de banda en bits por segundo y paquetes por segundo

o Reporte sobre protocolos
- Tabla que resuma el protocolo, dirección de In o Out, total y % de total, con valores actual, promedio y máximo

o Reporte sobre Tamaños de paquete:
- Tabla que resuma el tamaño del paquete, In, Out y total, con valores Actual, promedio y máximo.
- Gráfica de ancho de banda en bits por segundo y paquetes por segundo, dirección de entrada o salida versus el tiempo

o Reporte Alert Dashboard
- Tabla y gráfica que resuma la identificación del evento, la importancia, el impacto, la duración, hora inicio y fin, tipo y recurso

o Reportes sobre gusanos (Worms) y Dark IP
- Tabla que resuma el host y la tasa de transmisión

La Solución de Mitigación de Ataque de Negación de Servicios deberá contar con un sistema de gerenciamiento (consola de administración) centralizado que realiza aprovisionamiento basado en políticas, configuración de dispositivos, gerenciamiento de actualizaciones, monitoreo y control de los dispositivos involucrados.

La Solución de Mitigación de Ataque de Negación de Servicios deberá contemplar ser compatible con la mayoría de los correlacionadores de eventos comerciales disponibles en el mercado. Asimismo, se deberán de

proveer, integrados en el precio unitario de los servicios, los dispositivos (hardware, software e infraestructura auxiliar), que permitan que la solución de opere de acuerdo a los niveles de servicio solicitados.

7.2.1.9. **Solución de Prevención de Intrusos (IPS):**
Como se mencionó anteriormente, esta solución o capacidad se encuentra integrada al precio unitario de los Servicios Administrados de Seguridad de cada nodo.

El proveedor deberá ofrecer en esta solución, hardware de propósito específico que ofrezca, como mínimo, las funcionalidades descritas a continuación:

Generales:

- Debe permitir el paso del tráfico en el segmento de red sin afectar el funcionamiento de la red (Bypass)
- Debe tener la capacidad de soportar la alta disponibilidad en modos activo-pasivo y activo-activo. Además, debe soportar balanceo de carga internamente en el appliance.
- Debe tener la capacidad de soportar alta disponibilidad en modo de protección y simulación
- Debe de soportar el ruteo asimétrico, además de soportar el monitoreo de redes MPLS. Para su cumplimiento se aceptan cartas siempre y cuando vengan firmadas por el representante legal del fabricante, debiendo acreditar su personalidad.
- Debe de soportar el monitoreo de VLANs, incluyendo frames 802.1q y sensores virtuales internamente en el equipo.
- Debe de realizar un monitoreo transparente para los usuarios, donde de forma automática bloquee ataques maliciosos, preservando la disponibilidad del ancho de banda de red.
    - La solución debe soportar la detección y prevención de intrusos a servidores y a la red
- La solución no debe de requerir la modificación de los routers o switches funcionando como un puente en la red.
- Debe soportar el funcionamiento simulado; es decir, funcionamiento activo semejante al de prevención en línea, pero sin bloquear tráfico. El sistema sólo alerta qué eventos serían bloqueados.
- Debe permitir la creación de reglas y filtros de acceso. Los criterios necesarios son, al menos, poder aplicar reglas por adaptador, VLAN, protocolo, origen y destino.
- Soportar funcionamiento simulado: funcionamiento activo semejante al de prevención en línea, pero sin bloquear tráfico. El sistema sólo alertará sobre los eventos que serían bloqueados.
- Soportará la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo de forma simultánea, cuando se refiere a IDS (pasivo) quiere decir que es un IPS que puede funcionar en modo de captura de paquetes sin realizar acción preventiva alguna.

El posible proveedor deberá ofertar los IPS en base al ancho de banda máximo solicitado durante la vigencia del contrato.

Detección y de Bloqueo de Ataques:

- La solución debe de operar en la capa 2 del modelo de OSI y el monitoreo que detecte debe ser de:
    - Accesos no autorizados a los distintos recursos que se encuentren en la red
    - Ataques o violaciones en el uso de los recursos de red del IMSS
    - Violaciones a las políticas definidas
    - Intentos de acceso o firmas de ataque (attack signatures)
    - DoS, spyware, códigos maliciosos, gusanos, backdoors, aplicaciones P2P
    - Análisis de Active X que pueda descargar código malicioso previniendo "dialing home", se refiere a que el IPS pueda realizar análisis del tráfico de Active X que ejecutan los navegadores detectando así, cualquier código malicioso.

- Debe tener la capacidad de identificar y bloquear tráfico de aplicaciones instant messenger y P2P, con soporte mínimo para las aplicaciones con las funcionalidades mencionadas abajo:
  - AOL Instant Messenger: AIM File Transfer, Login, Mensaje enviado, contraseña cambiada, Inicio de cifrado de datos
  - MSN Messenger: MS Messenger Login, Mensaje enviado a un cliente
  - Yahoo Messenger: Yahoo transferencia de Archivos, loging, Mensaje enviado a un cliente, Yahoo messengerMessenger Chat
  - Gnutella, Gnutella conexión de un cliente, descarga de Gnutella, detección del cliente limewire
  - Kazaa, Kazaa Cliente detectado, descargas vía cliente FastTrack
  - eDonkey: Edonkey cliente detectado
  - BitTorrent: en intento de conexión, solicitud de GET un cliente
  - SoulSeek, SoulSeek detección del cliente al servidor
  - DirectConnect: Direct Connect estableciendo una conexión cliente servidor
  - Monitoreo de inspección tipo stateful
  - Interface de monitoreo en modo stealth, sin stack de TCP/IP en la interfaz
  - Detección de ataques independiente del sistema operativo

Se acepta que la solución IPS pueda identificar y en dado caso bloquear el tráfico P2P, independientemente de la aplicación utilizada.

- Debe de considerar al menos las siguientes tecnologías de detección y bloqueo de ataques:
  - Identificar el protocolo a partir del puerto utilizado (Port Assigment)
  - Identificar los protocolos que utilizan puertos aleatorios (Port Following)
  - Permite la identificación del protocolo usado en la mayoría de las conexiones que se inspeccionen (Análisis de contenido)
  - Identificación de protocolos, aun cuando éstos estén encapsulados (Protocol Tunneling Recognition)
  - Análisis heurístico
  - Análisis de protocolo. Con decodificación de al menos 165 protocolos y formatos de datos de la capa 2 a la capa 7 del modelo OSI, permitiendo la detección de ataques desconocidos o variaciones de ataques conocidos sin utilizar firmas. El proveedor debe entregar listado de los protocolos soportados e incluir al menos los siguientes: SIP, Compound Files, Java script, HTML, MSRPC, http.
  - DetecciónR de escaneo de puertos (Port Probes)
  - Permitir la detección de ataques desconocidos o variaciones de ataques conocidos a partir de firmas basadas en vulnerabilidades
  - ReensambladoRFC Compliance Checking - verificación de compatibilidad con las RFC's
  - Formatos de Archivos - identificar al menos 30 formatos de archivos. Algunos de los solicitados son: BMP, CAB, EXE, GIF, HTML, JAVA, MDB, SWF, URL, ZIP, MIME. Se entiende que las tecnologías de detección a lo que hace referencia dicho punto, se refieren al análisis de potenciales vulnerabilidades y código malicioso en los formatos de archivo mencionados.
  - TCP Reassembly - reensamblado de paquetes fragmentados
  - ReensambladoFlow Reassembly - reensamblado de sesiones fragmentadas
  - Debe tener la capacidad de analizar al menos los siguientes protocolos de VoIP: SIP, MGCP, Http Skype, H225 y H323
- Permitirá la detección de anomalías de tráfico a partir de análisis estadístico
- Permite firmas definidas por el usuario mediante el uso de regular expressions
- Presentará resistencia al menos a las siguientes técnicas de evasión:

- IP fragmentation
- TCP Stream Fragmentation
- RPC Fragmentation
- URL Obfuscation
- Mutación Polimorfica y Alteración del protocolo

- Deberá de proveer al menos los siguientes criterios de cuarentena:
  - Dirección del sistema víctima
  - Puerto del sistema víctima
  - Dirección del intruso
  - Puerto del intruso
  - Código ICMP
  - Tipo de ICMP
  - Duración de la cuarentena

Administración:

- Podrá administrarse de forma centralizada, a través de una sola consola del mismo fabricante, se deberá considerar, como parte de la oferta, una consola de administración.
- Debe soportar la integración de Syslog (número ilimitado de dispositivos)
- Deberá soportar el ajuste dinámico de severidad en los ataques, como resultado de la correlación de eventos
- Deberá soportar la correlación de datos de vulnerabilidades
- Deberá soportar la comunicación de datos en forma cifrada
- Deberá generar reportes en formato texto y gráfico, con exportación a formatos HTML, PDF y CSV
- Capacidad de envío de eventos como mínimo por SNMP
- Deberá soportar la administración remota vía Web con interfaz gráfica, para el uso en modo de consulta de dispositivos y eventos de seguridad
- Poder realizar de manera remota y automática su actualización y configuración de políticas
- Deberá soportar la creación de múltiples roles, en el cual se permita o niegue el acceso a los diferentes dispositivos, o se den y revoquen privilegios para la administración, visualización de eventos y generación de reportes
- Debe tener la capacidad de poder realizar automáticamente actualizaciones de software vía remota o Web para asegurar una protección en tiempo real. Las actualizaciones aplicadas no deben requerir de la reinicialización del componente habilitador
- Incluirá una Base de datos de soporte (knowledge base) accesible a través de Internet que contenga una base de datos de referencia con cada una de las nuevas vulnerabilidades descubiertas, para ser analizadas y estudiadas como futura referencia

7.2.1.10. **Servicio de Firewall:**

Como se mencionó anteriormente, esta solución o capacidad se encuentra integrada al precio unitario de los Servicios Administrados de Seguridad de cada nodo.

El proveedor deberá ofrecer en esta solución, el hardware y/o software necesario que cuente con las siguientes características y que ofrezca las funcionalidades descritas a continuación:

Generales:

- Posibilidad en modos de operación transparente y gateway
- Soporte a enlaces redundantes para Alta Disponibilidad o balanceo de cargas, tanto para conexiones en texto claro como cifradas dentro de VPN de manera nativa en el firewall

- Contar con la capacidad de soporte en Alta Disponibilidad de al menos activo-pasivo y activo-activo, es decir, sin pérdida de conexiones en claro, cifradas, o clasificadas por el QoS, en caso de que un nodo falle
- Contar con soporte a Balanceo de cargas entre gateways de Firewall/VPN/QoS
- Soportar los protocolos SNMP RFC 1157, SNMPv2c o SNMPv3
- Contar al menos con una de las siguientes certificaciones:
  o ICSA
  o Common Criteria EAL3+ o superior
  o FIPS 140 –Level 2 o superior
  o TISEC E3
- Soportar al menos las siguientes tecnologías de red: Ethernet, Fast Ethernet, Gigabit Ethernet
- Soportar ruteo dinámico (por lo menos OSPF, BGP y RIP)
- Contar con la capacidad de hacer NAT estático (uno a uno); así como dinámico (muchos a uno), configurables de forma automática (solo especificando IP fuente e IP traducida)
- Contar con soporte a NAT para VoIP (tecnología de Voz sobre IP)
- Soportar la tecnología de QoS basada en colas inteligentes. Se requiere son funciones de QoS como: Encolamiento de prioridad, para tráfico que no puede tolerar latencia. Encolamiento jerárquico de prioridad (para crear una cola de tráfico prioritario dentro de otra cola)
- Soportar el monitoreo gráfico en tiempo real del tráfico de QoS que está circulando por el dispositivo directamente en el equipo Firewall o en el equipo CPE.
- Capacidad de poder hacer administración de Ancho de Banda por IP fuente, IP destino, dirección (hacia adentro o hacia fuera), URLs definidos por el usuario y horario
- Capacidad de hacer administración de ancho de banda por usuario o grupos de usuarios
- Soporte a límites (máximo ancho de banda a usar), garantías (mínimo reservado) y pesos relativos (prioridades) como acciones para el tráfico clasificado. Limitar o bloquear otras aplicaciones intensivas en su consumo de ancho de banda para otorgar más espacio en ancho de banda para aplicaciones críticas de negocio del Instituto, es la acción mínima para garantizar la priorización del tráfico clasificado.
- Analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs
- Especificar políticas tomando en cuenta puerto físico fuente y destino
- Definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.
- Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando
- Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)
- Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos
- Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)
- Capacidad de hacer traslación de direcciones estático, uno a uno, NAT
- Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT
- Capacidad de bloquear equipos y ponerlos en cuarentena cuando estos no cumplen con políticas de seguridad o son identificados como generadores de tráfico malicioso

- Proporcionar protección y soporte al menos a las siguientes tecnologías de Voz sobre IP: SIP, H.323, MGCP y SCCP (Skinny) para tráfico cifrado y calidad de servicio
- Capacidad de poder hacer filtraje dentro de puertos TCP conocidos, aplicaciones potencialmente peligrosas como P2P aun y cuando se haga "tunneling" de estos simulando ser tráfico legítimo del puerto
- Soporte a aplicaciones Web y sus mecanismos de comunicación, tales como XML/SOAP.
- Debe soportar al menos los siguientes servicios: DCE RPC de Microsoft, NFS y SQL
- Capacidad de protección de tráfico de correo basándose en los tipos MIME en los archivos anexos (attachments), rechazar código ActiveX o Java, verificación de cumplimiento de los RFC relevantes; y que se tomen medidas para prevenir negación de servicio, tales como el máximo número de receptores, tamaño máximo de mensaje y máximo número de comandos erróneos

VPN seguras:

- Poder tener integrada una solución de VPN, por si se planea adicionar soporte a VPN posteriormente
- Realizar configuración central de todos los dispositivos de VPN, sin que sea uno a uno.
- Soporte para esquemas VPN site-to-site en topologías "Full Meshed" (todos-contra-todos), Estrella (oficinas remotas hacia una oficina central), "Hub and Spoke" (tráfico entre oficinas remotas, pasando por inspección central), además de VPNs client-to-site (VPNs de Acceso Remoto)
- Capacidad de establecer VPNs entre nodos remotos con IP dinámica en topologías estrella y malla
- Soporte integrado para VPNs sin cliente mediante SSL, permitiendo flexibilidad en la comunicación VPN desde equipos a los que no pueda instalársele un cliente.
- Soporte para que se puedan establecer VPN usando clientes tipo L2TP
- Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.
- Se deben soportar longitudes de llave para AES de 128, 192 y 256 bits
- Se deben soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14
- Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256
- Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site
- La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN). Es solvente la propuesta que habilite la funcionalidad "interface-mode VPN" referenciada bajo un nombre distinto.
- En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall
- Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS XSoporte a que los clientes de VPN puedan ser integrados con firewall personal (usando el mismo software) y verificador de configuración, con política administrada centralmente por la misma consola de la VPN. Los clientes de VPN que se propondrán podrán verificar la existencia de un firewall personal en la máquina cliente, mas no deben forzosamente tener la capacidad de la gestión de la solución de firewall personal.
- Debe tener capacidad de soportar VPNs cliente-a-sitio (client-to-site) basadas en SSL, que sean iniciadas en cualquier equipo que cuente con browser compatible y que sean terminadas en el gateway de VPNs
- Debe de soportar las VPNs SSL debiendo ser capaz la solución de verificar la legitimidad del cliente remoto efectuando un escaneo del equipo pudiendo detectar aplicaciones maliciosas como malware y spyware impidiendo el acceso del usuario en caso de que se detecten dichas aplicaciones
- Las cantidades correspondientes por tipo de tunel (IPSec, SSL) deberán ser soportados por la solución son IPSEC al menos 1000, SSL al menos 50.
- Para una mayor escalabilidad y facilidad administrativa, contención de fallos, a propuesta del posible

proveedor, siempre y cuando cumpla con lo establecido en el numeral de referencia y los niveles de servicio podrá utilizar equipos separados de la solución de firewall para las funciones de VPN. Incluso, dada las diferencias de características entre un tunel sitio-a-sitio (IPSec) y un tunel cliente-a-sitio, es posible separar el tráfico de estos dos tipos de túneles, por lo que se aceptan propuestas en donde el equipo Firewall haga las funciones de VPN y las propuestas donde el equipo VPN sea distinto al equipo Firewall.

Administración:

- La solución de Firewall deberá de administrarse de forma centralizada a través de una sola consola de administración y monitoreo de políticas de firewall, VPN y QoS, en un solo equipo central con funcionalidades de monitoreo en tiempo real y reporteo
- La consola de administración debe tener la capacidad de definir administradores con diversos roles, con distintos permisos dentro de la consola para poder delegar funciones administrativas
- Debe de soportar la autenticación fuerte (certificados) de manera nativa en la solución, para los administradores de la consola. Bajo el entendido de que una autenticación fuerte se logra bajo la integración con servidores de One-Time Passwords (o Tokens) que operan con el protocolo RADIUS, se aceptan propuestas que logran la autenticación fuerte solicitada mediante la integración con servidores RADIUS, a propuesta del posible proveedor, siempre y cuando cumpla con lo establecido en el numeral de referencia y los niveles de servicio
- Debe de contar con la capacidad de dar seguimiento a los cambios realizados en la(s) política(s) de seguridad, de modo que sea posible revisar qué administrador hizo qué modificaciones, así como fecha, origen e impacto/alcance de la modificación
- Debe tener la capacidad de generar bitácoras, que permitan obtener fácilmente un reporte completo del estado de la seguridad en la red
- Debe contar con una Interfase gráfica de usuario (GUI), para hacer administración de la solución, además de una Interfase basada en línea de comando
- Deberá contar con una Interfase basada en Web para el acceso remoto considerando que la comunicación deberá de ser encriptada vía SSL al dispositivo firewall
- Tener la capacidad de poder realizar una integración transparente y certificada con directorios tipo LDAP
- Debe tener la capacidad de revisión de bitácoras en tiempo real
- Debe tener la capacidad de poder generar versiones de la política de seguridad, y poder regresar a versiones anteriores de la misma
- Debe tener la capacidad de monitoreo en tiempo real del tráfico circulando a través de los módulos administrados y monitoreo de sesiones, además de monitorear el estado de cada uno de los puntos de refuerzo (Firewalls, VPN's) que se encuentren en toda la red, en tiempo real
- Podrá realizar mediciones de conexiones por segundo, conexiones concurrentes y paquetes por segundo que están pasando a través del firewall y desplegarlas al usuario administrador en tiempo real desde la interfaz de administración (no mediante línea de comando). Bajo el entendido de que los paquetes por segundo es un dato importante, pero un dato que puede resultar más valioso es la medición throughput (Kbps) que pasa por el firewall,se aceptan propuestas de desplegar el throughput utilizado gráficamente o la gráfica de paquetes por segundo.
- Tendrá capacidad de generar reportes sobre el estado de los componentes, tráfico de red, y de las políticas de Firewalls, además de poder personalizar dichos reportes y de poder desplegar varios tipos de reportes en una sola ventana
- Tendrá capacidad para presentar reportes del estado de Túneles de VPN en tiempo real y en reportes históricos
- Permitirá graficación en tiempo real de los "top N" servicios más utilizados y de los equipos que están

consumiendo más ancho de banda
- Tendrá capacidad de generar acciones y/o alertas en función de determinados eventos como cambios de políticas o valores críticos en contadores como uso de al menos CPU, Memoria y Disco
- Tendrá capacidad de monitoreo y reacción sobre comportamiento de usuarios detectando actividades sospechosas, tales como intentos de acceso no autorizados permitiendo el bloqueo de las conexiones detectadas
- Tendrá capacidad de realizar actualizaciones centralizadas del software, de forma remota
- Realizar configuración central de todos los dispositivos de VPN, sin que sea uno a uno Tendrá capacidad de hacer actualizaciones de software de firewalls sin importar que la versión sea menos reciente que la actual versión de la consola de administración
- Tendrá capacidad de envío de eventos como mínimo por SNMP.

La solución de Firewall deberá contar con un sistema de gerenciamiento (consola de administración) centralizado que realiza aprovisionamiento basado en políticas, configuración de dispositivos, gerenciamiento de actualizaciones, monitoreo y control de los dispositivos de seguridad.

La solución de Firewall deberá ser compatible con la mayoría de los correlacionadores de eventos comerciales disponibles en el mercado y deberá operar de acuerdo con los Niveles de Servicio establecidos

7.2.1.11. **Servicio de Análisis de Flujo:**
Como se mencionó anteriormente, esta solución o capacidad se encuentra integrada al precio unitario de los Servicios Administrados de Seguridad de cada nodo.

El proveedor deberá ofrecer en esta solución los dispositivos necesarios que cuenten con las siguientes funcionalidades, mismas que permitan mostrar en tiempo real el flujo de tráfico de red del IMSS:
- Los cambios en el nivel de tráfico deberán ser detectados en comparación con el tráfico observado previamente
- Deben poderse detectar patrones de tráfico que sean diferentes a comportamientos predeterminados
- El servicio debe detectar escaneos lentos, rápidos, escaneos "stealth" y barridos de computadoras
- Debe poderse definir una política y detectar violaciones contra la misma
- Deben poderse detectar usuarios utilizando indebidamente recursos de red independientemente de dónde estos se hubieran logueado.
- El servicio debe permitir la detección de comportamientos de worm
- El servicio debe contar con actualizaciones de las últimas amenazas en Internet, comparar esas amenazas con el tráfico existente en la red y alertar con base en esas amenazas
- El servicio debe soportar al menos los siguientes formatos de flows:
  - NetFlow v5
  - NetFlow v7
  - NetFlow v9
  - sFlow v2
  - sFlow v4
  - sFlow v5
  - Juniper cflow
- El servicio debe interpretar ruteo asimétrico
- El servicio debe poseer un firewall propio para auto protección del mismo que rechace toda comunicación por default haciéndolo transparente a pings y host scans. Asimismo, siempre y cuando cumpla con lo establecido en el numeral de referencia y los niveles de servicio, se permite presentar propuestas que agregue un control de tráfico confiable dentro de la misma consola de administración

con el fin de proveer un bloqueo de tráfico por rangos de IPs, lo cual asegure que se rechaza toda comunicación no conocida / validada por el Instituto y logrando incrementar el nivel de seguridad de la solución.

- El servicio debe poseer un dispositivo central (analizador) que colecte flows, capturas de paquetes y los analice; así como dispositivos extras (colectores) que colecten flows, capturen paquetes y reporten al analizador.
- El servicio debe soportar un mínimo de 3 flows y 200 Mbps de captura de tráfico (modo sniffer)
- El sistema de detección de anomalías debe poder monitorear la tasa de tráfico de un determinado host/subnet y detectar cuando el tráfico exceda o sea inferior a niveles especificados. Estos niveles deben poder ser ajustados basados en la hora del día y el día de la semana
- El producto deberá poder ensamblar dos flows unidireccionales de distintos elementos de red y reensamblarlos en una sola conversación
- Las alertas de worms deben permitir crear una lista de los hosts infectados y detallar el tráfico de worm en ese puerto de aplicación, comparado con el tráfico que no es del worm en el mismo puerto de aplicación durante el mismo período de tiempo
- El producto debe poseer la habilidad de buscar las características de tráfico de un host, subnet, múltiples subnets o múltiples hosts y crear una política sobre ese tráfico. El sistema debe poder alertar cuando el tráfico difiere de la política
- El producto debe incluir ambas interfaces: consola local Gráfica y Línea de Comando
- La consola Centralizada podrá ser la misma para productos de IPS de red, IPS de servidor, correlación de eventos y elementos de escaneo de vulnerabilidades o independiente si las soluciones no son del mismo fabricante. Lo anterior siempre y cuando se cumpla con lo solicitado en las especificaciones técnicas y niveles de servicio
  Estas funcionalidades se deberán proporcionar a través del SOC.
- El producto debe poseer reportes que muestren los top 5,10, 20, 50 y 250 talkers de la red junto con la cantidad de tráfico que cada host consumió.
- El producto debe poseer reportes que muestren los top talkers que se comunican con un solo host o subnet en la red.
- Los reportes deben poder ser exportados a pdf, xml y csv.

La Solución de Análisis de Tráfico deberá contar con un sistema de gerenciamiento (consola de administración) centralizado que realiza análisis y reportes basado en políticas; gerenciamiento de actualizaciones.

Como se mencionó anteriormente, esta solución o capacidad se encuentra integrada al precio unitario de los Servicios Administrados. El proveedor deberá ofrecer en esta solución, el hardware y/o software necesario que cuente con las características y que ofrezca las funcionalidades solicitadas.

7.2.1.12. **Servicio de Control de Acceso a Páginas Web:**
Como se mencionó anteriormente, esta solución o capacidad se encuentra integrada al precio unitario de los Servicios Administrados de Seguridad de cada nodo.

El proveedor deberá incorporar en esta solución, el hardware y software o appliance de propósito específico que ofrezca las funcionalidades descritas a continuación:

- Deberá poseer más de 22 millones de URL's en la lista de sitios
- Las URL's deben estar clasificadas bajo más de 90 categorías y todas las categorías deben permitir bloquear o permitir el acceso, así como permitir el acceso con cuotas de tiempo, o permitir el acceso tras la aceptación de un término de responsabilidad
- Las URL's deben estar clasificadas según su contenido diario, es decir, en el caso de que el contenido

de una URL sea cambiado, el día siguiente ya deberá estar reclasificada bajo la categoría que refleje su nuevo contenido, para mantener la confiabilidad de la base de datos se requiere que sea actualizada por el mismo fabricante de la solución.

- Deberá poseer mínimo las siguientes categorías de URL's:
  - Banners y publicidad
  - Narcóticos
  - Sitios de almacenamiento personal de archivos y datos
  - Sitios de armas y municiones
  - Sitios de chateo por Internet
  - Sitios de compartido de archivos P2P
  - Sitios de compras y subastas
  - Sitios de contenido adulto o sexual
  - Sitios de contenido repulsivo
  - Sitios de descarga de MP3
  - Sitios de descarga de software gratis o pago
  - Sitios de hackers
  - Sitios de ilegales
  - Sitios de juegos o apuestas en línea
  - Sitios de mensajería instantánea
  - Sitios de phishing, spyware, adware, key loggers, inclusive aquellos sitios inocentes de otras categorías que hayan sido usados para hospedar phishing; luego de ser descontaminados, deben volver a sus categorías originales
  - Sitios Web potencialmente maliciosos basadas en la "reputación", más allá de las técnicas de filtrado tradicionales.
  - Sitios que despliegan zombies, (BOT Networks) que utilizan las redes internas para generar ataques de Negación de Servicio (DoS por sus siglas en Ingles), robo de identidad, robo de información, etc.
- Deberá identificar amenazas de seguridad, como spyware, spyware drive-by, bots y tráfico de redes bot, códigos maliciosos, phishing, pharming y keylogging; y bloquear el acceso en el gateway de Internet
  - Sitios de proxies públicos usados para evitar proxies corporativos (proxy avoidance)
  - Sitios de radio y televisión en línea
  - Sitios hacia los cuales los spyware, addware y keyloggers envían los datos recolectados de las victimas
  - Sitios o páginas de correo electrónico vía Web
  - Sitios personales y bloggers
  - Sitios que contienen video o audio (streaming), aunque pertenezcan a otra categoría, tal como noticias, deportes, etc.
  - Sitios sobre alcohol y tabaco
  - Sitios sobre violencia y terrorismo
- Deberá garantizar que nuevas páginas cuyo contenido represente riesgos a la seguridad sean agregadas automáticamente a la lista de URL's máximo cinco minutos después de haber sido descubiertas por el fabricante de la solución, durante el transcurso del día y de manera automatizada. Estas actualizaciones tendrán un registro del tipo de actualización que se llevó a cabo en función de las categorías, para mantener la confiabilidad de la base de datos se requiere que sea actualizada por el mismo fabricante de la solución.
- Deberá permitir la reclasificación manual de cualquier página Web según las necesidades, o bien permitir que ciertas páginas puedan ser accedidas en cualquier momento aunque pertenezcan a categorías bloqueadas

- Deberá permitir el ingreso de URL's o bien de Expresiones Regulares (RegEx) para reclasificación manual
- Deberá permitir el bloqueo de páginas que pertenezcan a categorías permitidas, pero cuya URL posea ciertas palabras "clave"
- Deberá permitir el acceso a páginas de ciertas categorías, pero bloquear el intento de ciertos tipos de archivo (tales como video, audio, archivos comprimidos, ejecutables, documentos, etc.) desde dichas páginas
- Los tipos de archivos deberán permitir la personalización por tipo de extensión del archivo, así como la creación de nuevos tipos de archivos, aunque no sean comúnmente encontrados en la Internet
- La consola de donde se realice la configuración/control/monitoreo podrá ser la misma que para los equipos IPS o independiente si las soluciones no son del mismo fabricante. Lo anterior siempre y cuando se cumpla con lo solicitado en las especificaciones técnicas y niveles de servicio.
- Deberá reconocer transparentemente a los usuarios de las siguientes maneras:
    - Usuarios de Dominios NT
    - Usuarios de Active Directory
    - Usuarios de Novell eDirectory
    - Usuarios LDAP autenticados por RADIUS
- Deberá pedir autenticación manual a aquellos usuarios que intenten navegar sin estar debidamente autenticados en el servicio de directorio, sin pedir autenticación manual a los demás usuarios. La herramienta puede tomar las credenciales del usuario para validar su rol en directorio activo si la herramienta ya se encuentra asociada y recibe información e interactúa con dicho directorio
- Deberá permitir la definición de una política general que aplique a aquellos usuarios que no tengan una política específica asignada
- Deberá permitir diferentes tipos de bloqueo por horarios del día y días de la semana para cualquiera de las políticas definidas, el Instituto requiere bloqueo por horarios del día y días de la semana para cualquiera de las políticas definidas.
- Deberá permitir la definición de montos de cuotas de tiempo distintos para usuarios de grupos distintos, para usuarios específicos y para los usuarios generales
- Deberá exhibir una página HTML personalizable cada vez que un usuario intente acceder a una página bloqueada
- Deberá pedir confirmación al usuario cada vez que sea necesario usar su cuota de tiempo para navegar hacia cualquier página que pertenezca a una categoría que haya sido definida como permitida con el uso de las cuotas de tiempo a través de una página HTML personalizable.
- Permitir a los usuarios acceder a sitios controlando el tipo de operaciones que pueden ejecutar para evitar riesgos relacionados a consumo de ancho de banda, productividad en los empleados o fuga de información.
- Habilitación de búsquedas seguras en motores de búsqueda, incluyendo multimedia en los buscadores como "Ask", "Google", "Yahoo", "Bing", "Lycos", "YouTube"
- Permitirá control granular sobre redes sociales y sus aplicaciones como: "publicar mensajes", "enviar email", "email", "subir fotografías", "subir videos", "juegos", "mensajería instantánea". En sitios como: Vkontakte, Twitter, Sina, MySpace, Linkedin, Friendster, Facebook, Classmates, Bebo, Odnoklassniki, Google Plus, Orkut, RenRen, Mixi, entre otros, será suficiente demostrar que se cuenta con el control granular sobre redes sociales y/o Web2.0, y que los sitios mencionados son meramente informativos.
- Permitirá control de correo electrónico Web, Clips de Audio y video, Mensajería instantánea Web, y aplicaciones Web generales. Así mismo, los controles granulares por cada tipo de aplicación como "Enviar correo", "Subir archivo anexo", "Descargar audio", "Descargar video", "Subir video", "Play sobre video", entre otros.
- Permitirá la definición de políticas en las cuales ciertos usuarios puedan usar sistemas de Mensajería

Instantánea libremente; otros usuarios no puedan usar sistemas de Mensajería Instantánea, y ciertos usuarios los puedan usar, pero al intentar enviar o recibir cualquier archivo adjunto, deberán ser bloqueados

- Deberá permitir la definición de políticas de uso de Protocolos por IP, rangos de IP's, usuarios y grupos de los siguientes servicios de directorio:
  - Dominios del Microsoft Windows NT (NTLM)
  - Dominios del Microsoft Active Directory
  - Directorios LDAP
  - Directorios Novell eDirectory
    - Deberá reconocer transparentemente a los usuarios dePing Sweep
    - Pruebas UDP (User Datagram Protocol)
    - Huella del dispositivo
    - Descubrimiento rápido
    - Descubrimiento por NetBIOS
    - Descubrimiento por TCP (Transfer Control Protocol)
    - Descubrimiento de Puertos UDP
    - Identificación de Sistema Operativo
    - Identificación de la Aplicación

En lo que se refiere a los directorios de Novell, será suficiente con demostrar la compatibilidad del directorio activo basado en Novell

- Deberá contar con al menos las siguientes maneras, integradas al filtrado HTTP:
  - Usuarios de Dominios NT
  - Usuarios de Active Directory
  - Usuarios de Novell eDirectory
  - Usuarios LDAP autenticados por RADIUS
- El mecanismo de mantenimiento deberá permitir la programación de tareas automáticas para horarios predefinidos
- El mecanismo de mantenimiento deberá ser accesible desde la Web
- Deberá poseer interfaz de generación de reportes basados en templates predefinidos, los cuales deberán permitirse el filtrado por usuarios, grupos de usuarios, categorías, clases de riesgos, acción tomada por el sistema, fechas y rangos de fechas
- La interfaz de generación de reportes deberá permitir a personal autorizado la generación de resúmenes, reportes detallados, gráficas y tablas sencillas
- La interfaz de generación de reportes deberá permitir exportarse los reportes generados para mínimo los siguientes formatos:
  - Microsoft Word (Opcional)
  - Acrobat PDF
  - HTML
  - CSV
- La interfaz de generación de reportes deberá permitir la programación de múltiples tareas de generación de reportes predeterminados, en horarios y días de la semanas predefinidos, y deberá:
  - Enviar los reportes generados por correo electrónico hacia los recipientes deseados
  - Publicar los reportes generados en una página de la Intranet
  - Copiar los reportes generados hacia una carpeta local o en la red
- Deberá poseer interfaz de acceso directo a los registros de log a través de la Web, utilizando el concepto de drill-down
- La interfaz de acceso directo a los registros de log deberá permitir que cada criterio de datos se pueda

expandir según otro criterio, generando informes de múltiples niveles

- La interfaz de acceso directo a los registros de log deberá permitir que cualquier pantalla de visualización se pueda exportar para archivos de Microsoft Excel o bien para el formado Adobe Acrobat PDF
- La interfaz de acceso directo a los registros de log deberá permitir la personalización de los reportes generados
- Se podrá generar reportes de Riesgos de Seguridad presentes, como que usuarios/IP han sido atacados con Spyware, Phising, Addware, Keyloggers, etc.
- Se generarán reportes en función de cuánto ancho de banda consumen estas clases de riesgos (bytes Enviados/Recibidos/Total)
- Estos mismos reportes de riesgos, tendrán información que permitan hacer análisis forense para poder identificar y erradicar dichos riesgos
- Se podrá configurar que se manden dichos reportes por correo de manera periódica
- Se podrá configurar que se envíen alertas en tiempo real, a correo electrónico o en pantalla, sobre estos riesgos, a detalle, con información sobre Usuario/IP, Categoría accedida, Sitio/URL, IP del Sitio, la disposición (si fue bloqueada o permitida de acuerdo a las políticas), hora y fecha
- La interfaz de acceso directo a los registros de log deberá permitir la generación automática de reportes y su distribución por correo electrónico

La solución de Control de Acceso a páginas web deberá contar con un sistema de gerenciamiento (consola de administración) centralizado que realiza aprovisionamiento basado en políticas, configuración de dispositivos, gerenciamiento de actualizaciones, monitoreo y control de los dispositivos.

El posible proveedor podrá ofertar una solución que integre ambas funcionalidades Firewall, IPS y control Control de Acceso Web, siempre y cuando cumpla con los niveles de servicio requeridos.

7.2.1.13. Portal de Información Preventiva ante Vulnerabilidades Detectadas en Internet

Esta solución o capacidad se encuentra integrada al precio unitario de los Servicios Administrados de Seguridad de cada nodo.

El proveedor deberá contar para la administración y prevención de incidentes en Internet con un Portal que muestre el comportamiento del tráfico actual en Internet con respecto al histórico, así como alertas o avisos de seguridad. Este portal debe ser accesible tanto para sus propios operadores del servicio como para al menos 5 usuarios concurrentes definidos por el IMSS, a su vez el acceso será desde la red interna e internet.

El Portal de Seguridad debe contener lo siguiente:

- Vista en una gráfica de las últimas 24 horas de la utilización de la red de Internet (en bytes o conexiones o una combinación de ambos) del proveedor, por tipo de tráfico o aplicación, así como una proyección de la utilización para las próximas 6 horas y un comparativo contra la utilización histórica. Esta vista deberá ser utilizada para identificar y detectar de forma temprana cualquier actividad inusual del tráfico en Internet. El tipo de tráfico o aplicación a monitorear para su utilización son:
  - Peticiones / respuestas de protocolo web (HTTP /HTTPS)
  - Aplicaciones punto a punto (FTP, P2P)
  - Infraestructura (p. ej. ICMP, DNS, protocolos de ruteo)
  - Mensajería (SMTP, POP, IMAP, IRC etc.)
- Utilización actual (por hora) de la red de Internet para los puertos más utilizados del protocolo TCP, UDP, ICMP e IP con un comparativo de la utilización actual contra el valor histórico para la misma hora del último mes.

- La capacidad de presentar la utilización (en flujos, bytes o paquetes) de forma gráfica con respecto al total del tráfico para cualquier puerto de TCP o UDP para diferentes rangos de tiempo (hora, día, o semana en curso).
- Generación por parte del usuario de reportes de utilización por puerto de protocolo TCP, UDP, ICMP e IP para un periodo de tiempo definido (último mes).
- Los reportes de utilización de puertos generados por el usuario deben desplegar las alertas de seguridad o avisos generados para ese puerto en particular.
- La utilización de puertos por las aplicaciones por protocolo de transporte como TCP y UDP (puertos del 0-65535) o tipos para ICMP (tipos del 0 al 255), medida en flujos con respecto al total de flujos del protocolo (TCP,UDP o ICMP) debe considerar para cada puerto lo siguiente:
    - Utilización actual de flujos del puerto en porcentaje con respecto al total del protocolo
    - El promedio de utilización histórico de las últimas semanas (3 a 5 semanas) del puerto con respecto al total para el protocolo.
    - Factor de cambio de la utilización actual con respecto al histórico.
- El portal debe presentar alertas de eventos de seguridad en la red de Internet basadas en monitoreo del tráfico, del análisis y la correlación con vulnerabilidades conocidas. Las alertas deberán estar clasificadas por tipo o severidad con al menos 3 niveles o tipos:
    - Alerta comprobada (para un incremento de tráfico asociado a una vulnerabilidad o ataque, puede causar un daño potencial y requiere una acción).
    - Advertencia (para un incremento de tráfico inusual sin asociación a un ataque).
    - Advertencia Limitada (para detección de ataque en algún punto focalizado de la red de Internet, pero que se traduce en un mal comportamiento generalizado en la red).
- Las alertas de seguridad deberán contar con recomendaciones asociadas de actividades de contención y/o erradicación. Por ejemplo, bloqueo de tráfico de ciertos protocolos, o aplicación de parches para sistemas.
- Las alertas deben tener asociada una vista del tráfico en el momento de su generación para el puerto específico afectado y mantenerla como referencia histórica.
- El portal deberá mostrar avisos de seguridad. Los avisos de seguridad son advertencias de amenazas nuevas o preexistentes sobre servicios (DNS/HTTP/HTTPS) o sobre vulnerabilidades reportadas en productos o plataformas específicas por parte de proveedores. Los avisos de seguridad deben cubrir tecnologías comunes para su rápida identificación como:
    - Microsoft Windows/DOS
    - Solaris/ Sun OS
    - Peoplesoft
    - IBM AIX
    - Cisco IOS
    - Bases de datos
    - APPLE
    - Oracle
    - Unix
    - Email
    - Seguridad/Firewall
    - Linux
    - Correo
    - Equipo Genérico de Red
- La información resumida de los avisos de seguridad debe contener al menos: Fécha de publicación, descripción o resumen, ID dentro del portal, proveedor.
- La información detallada de los avisos de seguridad deben contener la siguiente información

El Instituto requiere que se notifique al personal que éste designe, cualquier pérdida de disponibilidad y recuperación con base en los puntos que se adjuntan a continuación. En caso de que el personal del IMSS no pueda ser localizado vía telefónica, el proveedor deberá enviar en paralelo un mensaje de voz, un mensaje SMS al celular del contacto y un correo electrónico.

- Si el servicio no responde en el intervalo de poleo, se deberá enviar otros tres intentos dentro de los siguientes 120 segundos.
- En caso de que no se haya restablecido la disponibilidad, el Instituto requiere que se compruebe la pérdida del servicio de forma manual a través de un enlace independiente al utilizado por la herramienta de monitoreo.
- En caso de comprobar la no disponibilidad del servicio, se deberá notificar al personal designado por el IMSS.
- En el momento de que se detecte la recuperación y estabilización del servicio, por al menos 30 minutos, se debe notificar al personal designado por el Instituto.

El Instituto requiere que los registros de la herramienta se almacén por al menos un mes en el repositorio de información del servicio y deberán ser entregados, en formato electrónico, cuando el MSS los requiera. Asimismo, el Proveedor debe generar de forma mensual un reporte con la siguiente información: 1) página monitoreada (dominio y dirección IP), 2) descripción de los problemas de indisponibilidad presentados en el período y 3) tiempo promedio de indisponibilidad.

Es importante destacar que no se aceptan soluciones de software libre, distribución gratuita, código abierto o sin soporte del desarrollador (fabricante).

7.2.1.15. Servicios Operativos

A continuación, el IMSS describe los distintos Servicios Operativos que serán indispensables para complementar adecuadamente los servicios administrados de Red Privada Virtual, Internet, por lo que deben ser considerados integrales y homologados a los mencionados.

Todas las labores de servicios y operación descritas a lo largo del presente anexo técnico, tales como: soporte técnico, optimización, mantenimiento preventivo y reactivo, puesta a punto, ajustes finos, mejoras, actualizaciones de hardware, software, firmware y firmas de seguridad, altas, cambios, bajas de configuraciones, análisis de fallas, análisis de desempeño, auditorías y demás servicios requeridos para la correcta operación de los Servicios, así como el cabal cumplimiento de los Niveles de Servicio Requeridos para cada uno de los Servicios estipulados en este documento de Anexo Técnico y todas sus Secciones, serán consideradas como parte de los precios asociados a la provisión de sus respectivos Servicios Administrados (RPV e Internet). El IMSS no incurrirá en ningún costo adicional por los Servicios de Operación descritos en este Anexo Técnico, y bajo ninguna circunstancia ejercerá una erogación adicional asociada a los Servicios de Operación aquí descritos, ni mediante unidades de servicio desagregadas, soporte extendido, ni cualquier otro mecanismo de pago alterno y/o adicional.

Servicios de Monitoreo y Gestión

El proveedor deberá tener la infraestructura y herramientas de monitoreo necesarias que permitan conocer el estado que guardan todos los componentes, infraestructura, equipos, enlaces y servicios que integran los servicios descritos en este Anexo Técnico, independientemente de la configuración de equipos y funcionalidades que tengan cada uno de los nodos del IMSS, así como la capacidad de personalización de la información tanto en su presentación visual, como en los reportes que serán generados. Las herramientas mencionadas son parte de un servicio integral que se puede componer de más elementos conforme a la estrategia que oferte el posible proveedor.

El proveedor deberá ofrecer la gestión del servicio de forma pro-activa, es decir, anticiparse a los problemas e incidentes que se puedan presentar durante la vigencia del contrato, vía el cumplimiento de los Niveles de Servicio establecidos; además dicho servicio debe estar diseñado para proveer el conocimiento del desempeño de los componentes de datos, video y voz en la RPV y en su seguridad.

El servicio deberá proporcionarse de forma remota desde las instalaciones del proveedor, considerando redundancia a nivel de enlaces, además de contar con todos los recursos necesarios para la prestación del servicio los cuales aseguren el funcionamiento de la infraestructura habilitadora, parte del alcance de la presente contratación, en un esquema 7x24x365 y durante la vigencia del contrato. De igual manera, deberá considerar el personal de apoyo en sitio que se requiera, para cumplir con los niveles de servicio establecidos y para proporcionar la continuidad de la operación que requiere el IMSS.

El proveedor será el responsable de realizar en su totalidad la gestión del servicio, en todos los sitios; debiendo considerar al menos lo siguiente:

- Líder de Gestión del Servicio
- Mesa de Servicio
- Administración de problemas
- Administración de la configuración
- Administración de cambios
- Administración de los niveles de servicio
- Administración de las plataformas
- Monitoreo de las plataformas
- Mantenimiento de las plataformas
- Actualización de las plataformas

Administración y Monitoreo

El proveedor se obliga a efectuar la administración y monitoreo de toda la infraestructura (Redes WAN, Internet y Seguridad), incluyendo gestión proactiva del aseguramiento del servicio, conociendo de manera preventiva los diferentes indicadores de niveles de servicio de la red en datos en todos los sitios a nivel nacional. Esta gestión deberá realizarse de manera centralizada libre de costos adicionales al IMSS, con accesos seguros, como VPN, IPsec, SSH o HTTPS.

Se entiende que este monitoreo es proactivo y que todo el seguimiento debe ser con los procesos automáticos, definidos por el proveedor y el Instituto en las mesas de trabajo, de tal forma que se cubran las funcionalidades y niveles de servicio solicitados.

El monitoreo deberá proporcionar lo siguiente:

- Acceso vía web a los reportes generados por el sistema de monitoreo a través de cualquier PC bajo control del IMSS y se deberán considerar 5 (cinco) accesos simultáneos.
- Monitoreo en Tiempo Real de los componentes de acuerdo a los tiempos de muestreo acordados entre el Proveedor y el Administrador del Contrato para la obtención de datos de la infraestructura, equipamiento, ruteradores, enlaces, servicios agregados como lo son los relacionados con la seguridad (firewall, IPS, etc.), y el demás objeto de la presente contratación
- Extracción e interpretación de datos relacionados con el estado y el desempeño de los dispositivos que componen a la RPV y servicios agregados como lo son los relacionados con la seguridad (firewall, IPS, etc.) y el demás objeto de la presente contratación

- Número de control
- Asunto
- Clasificación
- Proveedor
- Producto
- Puertos
- Protocolo
- Fecha
- ID de Alerta del producto
- Número de Parche
- Sistemas vulnerables
- Resumen de la vulnerabilidad

- Se considera deseable que el portal de seguridad pueda ser accesible en forma segura (acceso duro) desde un dispositivo externo tipo smartphone o tablet, siempre y cuando el dispositivo sea accesible de acuerdo a las especificaciones establecidas en el anexo.
- *Es importante destacar que no se aceptan soluciones de software libre, distribución gratuita, código abierto o sin soporte del desarrollador (fabricante).*
- *El Instituto requiere gráficas de lo descrito en cada una de las funcionalidades mínimas solicitadas, siempre y cuando no impacte en los servicios solicitados.*

El portal con la Información de Seguridad en Internet deberá contar con las siguientes funcionalidades:

- Disponibilidad del Portal de Seguridad de 7x24x365.
- Mostrar la información en inglés o español. El idioma podrá ser configurable en el portal o en el navegador.
- Autenticación del usuario mediante usuario y contraseña para el acceso a la información. Se requiere autenticación para el acceso a la información, exclusivamente.
- Ligas (hipervínculos) hacia otros sitios de seguridad relevantes. Los sitios mínimos a los que deberá apuntar podrán ser sitios de los fabricantes de su propuesta técnica, Centros de Respuesta a Incidentes, security focus, osvdb, secunia, cert.org, zone-h, cve.mitre.org. Los anteriores sitios deberán ser considerados como enunciativo más no limitativo.
- Explicación de alertas de forma detallada con apoyos multimedia cuando sea posible
- Noticias recientes de la industria sobre seguridad de información o recomendaciones de buenas prácticas de seguridad por parte de expertos en el tema. El posible proveedor adjudicado deberá de alimentar la información, y será visible en el portal y enviadas por correo.
- Desplegar el nivel de alerta de la red de Internet alineado con la escala de colores de Homeland Security Advisory System de los Estados Unidos: Verde = Bajo, Azul =En Guardia, Amarillo = Elevado, Naranja =Alto, Rojo = Severo, Gris = Normal (sólo valido para tráfico)
- Una vista rápida de resumen alertas, avisos o utilización de puertos y ligas hacia reportes detallados
- La vista rápida de alertas debe tener una descripción de las alertas más severas, asunto, fecha y resumen y desplegarlas en orden cronológico. El usuario debe tener la capacidad de ordenarlas o realizar búsquedas por Fecha, ID o Descripción
- La vista rápida de avisos debe contener al menos asunto, fecha, vulnerabilidad y resumen, ordenados de forma cronológica. El usuario debe tener la capacidad de ordenar o realizar búsqueda de avisos de seguridad por fecha, por proveedor, o por tipo o por descripción
- La vista rápida de utilización de puertos debe contener al menos puertos de interés y su utilización actual (como porcentaje del total), utilización promedio histórica y factor de cambio entre la utilización actual y el promedio histórica.
- Los reportes detallados de utilización para un puerto específico deben tener asociados las alertas y

avisos para ese puerto.

- El usuario podrá configurar notificaciones por correo electrónico para cuentas específicas y establecer criterios para recibir tanto las alertas como avisos. El aviso por correo electrónico debe tener información suficiente para su valoración y una liga a la descripción detallada en el portal. La definición de alertas debe considerar:
  - Configuración por parte del usuario del nivel de alerta a configurar (alerta comprobada, advertencia o advertencia limitada)
  - Configuración por parte del usuario de alertas sólo de los puertos/tipos de interés para TCP, UDP, ICMP o IP.
  - Las alertas puertos de interés pueden configurarse de la siguiente manera:

    Para TCP y UDP:
    + Para todos los puertos (0-65535)
    + Para puertos bien conocidos (well known ports) (0—1023)
    + Para puertos registrados (0-49151)
    + Para puertos dinámicos (49152-65535)
    + Para puertos bajos (0-2047)
    + Subrangos

    Para ICMP:
    + Todos los tipos (0 a 255)
    + Tipos originales (0 a 16)
    + Tipos Extendidos (17 al 40)
    + No usados o experimentales (41 a 255)

- Configuración por parte del usuario de avisos sólo para ciertas plataformas o tecnologías, de tal forma que se reciban sólo sobre aquellas que son de su interés

7.2.1.14. Monitoreo a la Disponibilidad a servicios WEB

El proveedor, a través del SOC, deberá monitorear a través de un medio de comunicación diferente, independiente y externo a la red del Instituto, las páginas, sitios, portales o aplicaciones Web del Instituto publicados y visibles desde Internet; con la finalidad de verificar que están funcionando o estén alcanzables (activos y en condiciones normales de operación). En caso de que algún sitio o URL se inhabilite, no responda o trabaje inadecuadamente, se deberá alertar inmediatamente al personal que el Administrador del Contrato designe. Estas páginas o sistemas web tienen direcciones públicas iguales o similares al dominio "*.imss.gob.mx".

El monitoreo de disponibilidad a servicios Web del Instituto deberá ejecutarse de manera permanente durante toda la duración del contrato para hasta 20 sitios o URL´s que el Instituto indique al proveedor. Se requiere que el servicio de monitoreo se realice a través de una herramienta automatizada con la cual se verifique, en intervalos regulares, la disponibilidad del servicio HTTP/HTTPS para cada uno de los sitios definidos por el Instituto.

La herramienta de monitoreo deberá estar en el SOC del proveedor y éste deberá brindar el acceso a la herramienta vía HTTPS, mediante cuentas con rol de solo lectura, tanto de forma interna a la red del Instituto como de forma externa (a través de Internet).

El intervalo de poleo deberá ser inicialmente de 300 segundos para cada sitio.

Se entenderá como consola de monitoreo el acceso remoto vía http a las herramientas de monitoreo y gestión del NOC para el personal asignado por el IMSS.

Líder de Gestión del Servicio:
Para la gestión del servicio, el proveedor deberá designar un Líder, y en caso que lo considere conveniente supervisores, los cuales deberán ser notificados inmediatamente al Administrador del Contrato en caso de sustitución de personal.

Funciones mínimas del Líder:

- Deberá coordinar la ejecución del Sistema de Gestión del Servicio. (Operación Diaria).
- Consolidación y entrega de los reportes mensuales.
- Convocatoria y conducción de las reuniones de seguimiento mensuales y extraordinarias en la materia.

Funciones mínimas del Supervisor:

- Coordinar al personal en sitio para que se elaboren los trabajos encomendados por el Líder de Gestión del Servicio.
- Llevar una bitácora de trabajos y/o incidencias.
- Elaborar reportes de avance mensuales donde se muestre el estado que guarda el servicio prestado.
- Asistir a las juntas de coordinación que sean programadas por el personal del IMSS.

Herramientas de Monitoreo
Para la operación del monitoreo de los niveles de Servicio, el proveedor debe proporcionar la infraestructura que considere necesaria para asegurar la correcta medición de los niveles de servicio solicitados en el proyecto descrito en este anexo técnico.

Vale la pena reiterar que es responsabilidad del proveedor asegurar la correcta operación, dimensionamiento, soporte, gestión de dicha infraestructura para cumplir con los requerimientos y niveles de servicio establecidos en este proyecto.

De manera enunciativa, más no limitativa, algunas variables a monitorear en el servicio son:

- Disponibilidad
- Latencia
- Pérdida de paquetes
- Anchos de banda mínimos y máximos
- Porcentajes de utilización por enlace
- El crecimiento debe estar alineado con el crecimiento eventual del servicio hacia los máximos del contrato

El proveedor deberá operar el Portal Web de monitoreo de servicios requeridos que soporte diferentes usuarios con diferentes niveles de privilegios para que además de poder generar reportes de las KPI del Centro de Datos, estas puedan ser visualizadas a voluntad. La herramienta deberá entregar información en forma de reportes, variables, alertas y portales de modo que sea acorde a las mejores prácticas de ITIL. Las herramientas tanto de monitoreo y gestión, como de mesa de ayuda se podrá integrar y ofertar soluciones de distintos fabricantes que permita proporcionar la funcionalidad solicitada.

Como se mencionó anteriormente, las herramientas de monitoreo de niveles de servicio son del total responsabilidad del proveedor de servicios, desde su selección (siempre y cuando cumpla con al menos lo que se solicita en esta sección) hasta su puesta a punto, y será el encargado de darles el soporte adecuado para su correcto funcionamiento.

Entre las capacidades analíticas que se requieren para la herramienta de Gestión y Monitoreo de niveles de servicio para cada tipo de tecnología están al menos las siguientes:

Para los equipos: CPE

- Pruebas mínimas que debe poder realizar:
  - Pruebas de conectividad
  - Prueba de integridad de datos: Que se demuestre que los datos enviados de un nodo origen llegan sin alteración a un nodo destino.
  - Prueba de saturación de enlaces: Detectar que los enlaces están siendo saturados a su capacidad permitida por cierto tipo de tráfico identificado.
  - Pruebas de tiempo de respuesta
  - Prueba de loops: Demostrar que las redes de comunicación no estén conectadas físicamente de tal forma que generen problema de bucle que deterioren los tiempos de respuesta o que generen caídas.
- Utilidades mínimas que debe incluir
  - Ping
  - Traceroute
  - Tabla ARP
  - Tabla de enrutamiento
  - SNMP
- Métricas de desempeño mínimas que debe incluir el reporte obtenido de la herramienta
  - Utilización del ancho de banda
  - Throughput
  - Disponibilidad
  - Latencia
  - Paquetes perdidos
  - CPU de los Componentes Habilitadores del servicio tercerizado
  - Memoria de los Componentes Habilitadores del servicio tercerizado

Para los equipos de seguridad:

- Pruebas mínimas que debe poder realizar:
  - Pruebas de conectividad (ICMP)
  - Prueba de integridad de datos (ICMP)
  - Prueba de saturación de enlaces (Paquetes Perdidos)
  - Pruebas de tiempo de respuesta (Tiempos de ida y Tiempos de regreso)
  - Prueba de flujos TCP
  - Prueba de resolución de nombres (DNS)
  - Prueba de emulación de transacciones HTTP y HTTPS
- Utilidades mínimas que debe incluir
  - Ping
  - Traceroute
  - Escaneo de Puertos
  - SNMP
- Métricas de desempeño mínimas que debe incluir el reporte obtenido de la herramienta
  - Utilización del ancho de banda
  - Throughput
  - Conexiones por segundo

- Conexiones concurrentes
- Cantidad de traducciones NAT/PAT
- Disponibilidad
- Tiempo de respuesta
- Paquetes perdidos
- CPU
- Memoria

Se debe alinear con la disciplina de Help Desk de ITIL, entregando una cuenta de perfil de Monitoreo IMSS al personal de Mesa de Servicio para que éste pueda observar la misma información que fue causante de una alerta, además de dar el seguimiento hasta el cierre de ésta. Capacidades suplementarias a las disciplinas de Service Level Management de ITIL, Availability Management de ITIL y Capacity Management de ITIL.

Los reportes deben poder ser solicitados por medio del portal de gestión del servicio por los usuarios facultados, en cualquier instante del contrato, y pueden ser accesados a través de este, o pueden ser programados para su envió vía correo electrónico en el instante, o por periodos de tiempo previamente programados (diario, semana, mensual).

La herramienta debe permitir que se colecten métricas tipo NetFlows, sFlow y IP SLA de las infraestructuras de enrutamiento y conmutación de modo que se puedan a analizar los inventarios de Flujo de Información que la infraestructura pueda enviar a un colector centralizado en el Centro de Datos.

La herramienta de monitoreo de niveles de servicio, debe ser capaz de recibir el total de los flujos generados por el total de la infraestructura del servicio, dicha capacidad debe ser calculada por el posible proveedor como parte de su propuesta.

La herramienta de monitoreo permitirá la administración y controles de acceso de usuario, tales como:

- Manejo de perfiles de usuario.
- Dispositivos y secciones de la aplicación a los que puede acceder el usuario.
- Privilegios para la generación y consulta de reportes.
- Acceso a vistas de estado y desempeño de la red en tiempo real.

El proveedor debe mantener a punto la herramienta de monitoreo de niveles de servicio, proporcionando las mediciones continuas a la infraestructura y servicios a su cargo.

Deben de existir al menos las siguientes vistas que aseguraran cuales son las tecnologías que impactan cada uno de los grupos de elementos que componen el servicio objeto de esta contratación para cumplir con las acciones proactivas que garanticen la continuidad de la entrega del servicio:

- Vista donde se muestre el conjunto de variables tales como métricas de medición y disponibilidad de los enlaces, módulos de servicios, capacidades de infraestructura, variables que impactan un servicio, de modo que el impacto en una de ellas impacte el estado de la vista y de la posibilidad de drill–down
- Vista de mapa de los recursos y su relación para detectar por medio del drill-down las variables impactadas.
- Alarmas a nivel infraestructura para detectar el impacto que este tiene en los servicios.
- Alarmas a nivel de servicio para alertamiento a alto nivel de impacto a grupos de recursos.
- Alarmas de tipo seguridad, donde se muestre el tipo de ataque, el objetivo del ataque y la mitigación de éste.

Para garantizar que los eventos que se presenten sean manejados de la forma más eficaz, se deben entregar mensajes de alertas de la siguiente naturaleza:

- Vía Correo Electrónico
- Vía Traps SNMP para eventuales sistemas de gestión
- Capacidad de configurar y ejecutar Scripts de notificación
- Mensajes Texto o SMS

El proveedor debe configurar al menos una comunidad SNMP con derechos de lectura, independiente a la comunidad que él utilice para el monitoreo de los diferentes equipos de comunicaciones y seguridad controlados por él y que formen parte del servicio descrito en este anexo técnico.

Esta comunidad tendrá como objetivo monitorear todos estos equipos desde un sitio diferente al NOC, con uno o más servidores del IMSS (o un tercero definido por éste). En estos servidores se recibirá la notificación automática de incidentes y envío de traps SNMP, según parámetros establecidos por el IMSS, que permitan tener visibilidad sobre variables importantes de desempeño del servicio. En caso de que el IMSS lo requiera, el proveedor deberá proveer y configurar al menos una comunidad SNMP, sin menoscabo de agregar adicionales que no estén incluidas en este apartado. Las métricas que se requieren, ya sea por SNMP o MIBs, son las siguientes:

- Net Flow (SNMP, MIBs y/o solicitud por contrato) (Previa validación a través de una Mesa de Ingeniería IMSS-proveedor)
- IP Acc (SNMP, MIBs, y/o solicitud por contrato) (Previa validación a través de una Mesa de Ingeniería IMSS-proveedor)
- Logs
- Configuraciones
- Consumo de ancho de banda por enlace
- Niveles de Servicio de disponibilidad y desempeño establecidos en el contrato

Los registros generados por la herramienta o herramientas de monitoreo, serán los que se utilizarán para validar los niveles de servicio proporcionados por el proveedor, de acuerdo a los requerimientos del IMSS, y bajo los niveles de servicio definidos en la sección Niveles de Servicio de este anexo técnico.

- En caso de controversia, la información recibida a través del protocolo SNMP y MIBs en los centros de monitoreo del IMSS, podrá ser utilizada como referencia para determinar si existen diferencias respecto a lo reportado por el NOC del proveedor, y en su caso, ser reconocidas como elementos de juicio para establecer un punto de acuerdo. Esta opción solo será prerrogativa del IMSS y nunca del proveedor.
- Con el objeto de contar con la información para controlar y monitorear los servicios proporcionados, el proveedor debe proporcionar los reportes correspondientes al desempeño del servicio, información que debe de ser entregada dentro de los primeros 10 días hábiles del mes siguiente. Dependiendo de la importancia del reporte, de común acuerdo con el IMSS, se establecerán las fechas de los reportes identificados como críticos
- El proveedor debe realizar todas las configuraciones necesarias, para dejar habilitado el acceso a los equipos para poder recolectar los datos que le permitirán generar los reportes correspondientes.
- El Cuerpo de Gobierno del IMSS debe validar y permitir las configuraciones de acceso para la recolección de datos y para la presentación de reportes de acuerdo con las políticas de seguridad validadas por el personal facultado al interior del IMSS.

Centro de Operación de Seguridad (SOC)

Los posibles proveedores deberán ofrecer el monitoreo permanente de los elementos y servicios de seguridad solicitados durante la vigencia del contrato, con el fin de verificar el estado de cada uno de los elementos que lo soportan y tomar las acciones necesarias en caso de presentarse un evento que ponga en riesgo la operación del servicio. Para ello, el Posible proveedor deberá incluir en su Propuesta Técnica contar con un Centro de Operaciones de Seguridad (Security Operation Center, SOC, por sus siglas en inglés). El objetivo de este centro es el de la administración, supervisión, gestión y monitoreo de los elementos, servicios, soluciones y configuraciones de seguridad, mismas que deberán realizar análisis proactivo y reactivo con el fin de proteger las aplicaciones e información interna de la Institución.

El Instituto requiere que el posible proveedor oferte la integración de un programa de gestión de eventos conforme a los procesos y mejores prácticas de la industria de un SOC, a fin de proporcionar las funcionalidades y niveles de servicios solicitados.

La administración de la seguridad se deberá comandar desde este Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés). Será monitoreado y gestionado en su operación por el proveedor, en un régimen de 7x24x365, durante la totalidad de duración del contrato, y deberá contar con la cantidad de ingenieros necesarios para cumplir los acuerdos de nivel de servicio y horarios solicitados.

El SOC deberá estar suscrito a los principales sitios y listas de correo de Internet que notifican sobre nuevas vulnerabilidades. Cuando se detecte una nueva vulnerabilidad, el SOC deberá realizar inmediatamente un análisis para conocer si afectará las operaciones del IMSS en lo que a la infraestructura objeto del contrato atañe; y si es viable, iniciar los procedimientos aplicables así como emitir los boletines para difusión al interior del IMSS en coordinación con el Administrador del Contrato.

El SOC deberá contar al menos con dos procesos certificados en ISO/IEC 27001:2005 y deberá contar con al menos dos personas adscritas al SOC certificadas en ITIL V3 Nivel Intermedio OSA y RCV., las cuales brinden los servicios directos al Instituto.

Los alcances y funciones que tendrá el SOC durante la totalidad de duración del contrato serán, de manera enunciativa más no limitativa:

- Operar en un régimen de 7x24x365, durante la totalidad de duración del contrato, y deberá contar con la cantidad de ingenieros necesarios para cumplir los acuerdos de nivel de servicio y horarios solicitados.
- Dar atención hasta su resolución de los incidentes de seguridad presentados.
- Monitorear permanente las actividades realizadas en la red notificando al personal que designe el IMSS en máximo 30 minutos todas aquellas actividades sospechosas que puedan comprometer la seguridad.
- Monitorear el estado de operación de los componentes de la infraestructura tecnológica de seguridad, así como recolectar las alertas que generen, normalizar y correlacionar la información que de ellas se deriven y emitir los reportes que serán enviados a los responsables de seguridad del IMSS, de tal suerte que puedan manejar y responder a potenciales incidentes de seguridad o incidentes en curso a fin de tomar las medidas necesarias para contenerlos.
- Administrar la infraestructura de seguridad para mantener configuraciones óptimas a fin de asegurar la confidencialidad, integridad y disponibilidad de la información.
- Brindar el soporte para cualquier incidencia registrada por las herramientas y/o que le sea reportada.
- Actualización de memorias técnicas y documentos de control relacionados con elementos, soluciones y servicios de seguridad.
- Coordinación con otros recursos para atender casos de incidentes de seguridad de la Información.
- Reportar actividades sospechosas que puedan provocar un incidente de seguridad.
- Apoyar en el monitoreo y trazabilidad de paquetes para apoyar en la determinación de puntos de

indisponibilidad de servicios.

- Comunicar al personal que designe el IMSS cualquier incidente de seguridad y/o actividad sospechosa con base en lo establecido en el apartado "Prioridades de Seguridad2 descrito en este documento.
- Realizar con base a la autorización emitida por el personal del IMSS las actividades de contención para minimizar los impactos ocasionados por la presencia de una actividad sospechosa o un ataque.
- Establecer *Acuerdos* del Nivel de Operación (*OLA, por sus siglas en inglés*) con los terceros que el Instituto y los responsables de seguridad le indiquen.
- Resolver todas las fallas relacionadas con los dispositivos, soluciones y servicios de seguridad contratados, en coordinación con el personal de soporte en sitio y remoto solicitados en la sección correspondiente del presente documento "Soporte Técnico en Sitio y Remoto".
- Resolver todas las fallas relacionadas con los dispositivos, soluciones y servicios de seguridad contratado, basado en el modelo de gestión de fallas mencionado en la sección Atención a Fallas".
- Monitoreo de la salud de todos los dispositivos de seguridad habilitados para proporcionar los servicios y soluciones de seguridad considerando al menos: estado de la memoria, CPU, estatus de interfases y diferentes variables de los equipos
- Creación de reportes proactivos para los casos en que al detectarse o dispararse alguna alarma, se requiera especial atención, por ejemplo, violación de umbrales definidos de desempeño, caídas de interfases
- Notificación al personal que designe el IMSS en máximo 30 minutos, incluyendo el primer diagnóstico. El comunicado al cliente incluirá el evento detectado, así como las acciones a seguir y el estado del servicio (Severidad 1, Severidad 2, Severidad 3).
- Monitoreo en tiempo real de todos los dispositivos, soluciones y servicios de seguridad contratados.
- Capacidad para eventualmente interconectar el sistema de monitoreo del SOC, con un sistema designado por el IMSS, con el fin de acceder a información relativa a sus servicios con derechos de lectura.
- Capacidad para permitir al personal que designe el IMSS, para generar reportes explotando todas las variables y funcionalidades de la herramienta de monitoreo, con la opción de parametrizar dichos reportes y consultarlos vía Web.
- Notificación de las fallas de los servicios contratados al personal designado por el IMSS, por medio del proceso más apropiado (email, ticket de fallas, etc.)
- Soporte técnico en sitio o remoto para atender cualquier falla, incidente de seguridad o indisponibilidad de algún servicio del Instituto; debiendo ser permanente durante toda la duración del contrato cualquier día natural y en cualquier horario.
- Notificación inmediata al personal que designe el IMSS, al momento en que se detecte una falla en los dispositivos, soluciones y servicios de seguridad contratados, debiendo entregar un reporte detallado con la solución en un periodo no mayor a 12 horas, cuando éste sea solicitado por escrito por el IMSS. Para los casos donde el incidente sea motivo para ejercer una penalización o deductiva, el reporte Post-Mortem tendrá que ser generado en automático. Para los casos en los que el proveedor haya incurrido en penalización o deductiva, el reporte se entregará en automático, sin necesidad de que el Cuerpo de Gobierno del IMSS lo solicite.
- Base de datos que almacene íntegramente el historial de información de los dispositivos, soluciones y servicios de seguridad contratados monitoreado en forma diaria, con periodos de registro según se acuerden en las mesas de trabajo entre el proveedor y el Cuerpo de Gobierno del IMSS, y que permita conservarla para ser consultada en cualquier momento al menos durante los 60 días naturales posteriores a su generación, sin realizar ningún tipo de sumarización o compactación de los registros durante este periodo de consulta. Esta base de datos deberá almacenar dichos registros históricos en forma mensual, compactados, hasta la conclusión del contrato, y podrán ser solicitados por la Convocante en cualquier momento durante la vigencia del mismo. Los elementos a almacenar, así

como los mecanismos para su acceso, serán acordados conjuntamente entre el Cuerpo de Gobierno del IMSS y el proveedor en un plazo no mayor a 30 días posteriores a la fecha de notificación de fallo de la contratación.

- Medición de Capacidades: El SOC deberá llevar a cabo la contabilización de la utilización de los recursos de la infraestructura para proporcionar los servicios y soluciones de seguridad. Los sistemas de monitoreo recolectarán la información diariamente, para ser almacenada en una base de datos que deberá estar disponible en cualquier momento para que el personal autorizado del IMSS pueda revisar y generar los reportes, a través de aplicaciones proporcionadas o desarrolladas por el SOC.
- Generación de Estadísticas: En este punto el SOC deberá contar con aplicaciones que permitan generar, verificar y almacenar las estadísticas del desempeño, capacidad y utilización de cada uno de los elementos instalados para proporcionar los servicios y soluciones de seguridad, debiendo contar con un historial de los rubros descritos anteriormente; lo cual deberá tomarse en consideración para la elaboración de la planeación de capacidades (Capacity Planning). Este reporte deberá ser entregado de manera trimestral, y deberá tener, al menos, un análisis detallado del comportamiento de los servicios proporcionados, y las sugerencias de mejora basadas en este análisis.
- Estar suscrito a los principales sitios y listas de correo de Internet que notifican sobre nuevas vulnerabilidades. Cuando se detecte una nueva vulnerabilidad, el SOC deberá realizar inmediatamente un análisis para conocer si afectará las operaciones del IMSS en lo que a la infraestructura objeto del contrato atañe; y si es viable, iniciar los procedimientos aplicables así como emitir los boletines para difusión al interior del IMSS en coordinación con el Administrador del Contrato.
- Tener su propia gobernabilidad y por ende ser totalmente independiente del Centro de Operación de Red (NOC, por sus siglas en inglés)
- Contar con procedimientos detallados para la administración de incidentes, manejo de alarmas y análisis de información y correlación de eventos, por lo que deberá adjuntar copia simple de los mismos en su propuesta técnica. En caso de resultar el proveedor, los procedimientos serán revisados en conjunto con personal del IMSS, o quien éste designe, para hacer las adecuaciones particulares, en caso de aplicar.
- Llevar un estricto procedimiento de Control de Cambios que considere tener documentado toda adición, modificación, eliminación de las configuraciones, reglas y/o políticas de los elementos, servicios o soluciones de seguridad; esto con la finalidad de mantener una base y/o memoria técnica actualizada al día de las configuraciones que se tiene en los dispositivos.
- Generar y proporcional al personal que designe el IMSS siempre que sea requerido los archivos (con contraseña) que contenga los respaldos sobre las configuraciones, reglas y/o políticas, diagramas, especificaciones de todos los elementos, servicios o soluciones de seguridad

El Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) deberá cumplir con lo siguiente:

Requerimientos Mínimos del SOC:

Con objeto de contar con una adecuada Administración de la Seguridad, el posible proveedor tendrá que comprometerse, en su propuesta técnica, a cumplir durante la totalidad de duración del contrato con:

- El proveedor deberá contar con personal con experiencia comprobable en seguridad de información de 2 años como mínimo y con certificaciones en seguridad reconocidas.
- El proveedor deberá emplear metodologías reconocidas internacionalmente, basadas en mejores prácticas como ISSAF, CoBIT, ISO/IEC 27001:2005 e ITIL en la prestación de los distintos servicios de seguridad de información que se requieran para el alcance de esta propuesta.
- Las áreas que brindarán el servicio de SOC al IMSS, deberán estar certificadas en ISO/IEC 27001:2005 y en ITIL Management and Capability Level por lo menos.
- El proveedor deberá contar con un proceso o procedimiento de administración de riesgos que le permita

identificar y cuantificar riesgos y seleccionar los controles de seguridad correspondientes para garantizar los Niveles de Servicio acordados. Deberá identificar y describir brevemente dentro de su propuesta técnica el proceso de administración de riesgos (tales como OCTAVE o MAGERIT, por mencionar algunos) de seguridad de información utilizado en la prestación de sus servicios de seguridad de información.

- El proveedor deberá tener documentado e implementado un proceso de administración de incidentes de seguridad de información, así como la conformación de sus equipos de respuesta y administración de incidentes. Deberá describir brevemente, como parte de su Propuesta Técnica, los mecanismos que utilizará para determinar la causa raíz de los incidentes que podrían afectar la seguridad de la información de los servicios proporcionados, así como sus respectivos canales de comunicación y contacto con entidades mayores para la solución de los mismos.
- El proveedor deberá contar con la infraestructura exclusiva para el IMSS, necesaria para la administración, correlación, monitoreo y gestión de los dispositivos de seguridad incluidos en el contrato, siendo éstos de manera enunciativa más no limitativa, los Firewalls, IPSs, etc. Este servicio deberá estar incluido y dimensionado en cumplimiento a los requerimientos del presente contrato.
- El proveedor deberá contar con un programa de auditorías, a intervalos planeados, internas así como de terceras partes, para validar el cumplimiento que se tiene dentro de la empresa de políticas, proceso y procedimientos documentados como práctica regular asociadas con los servicios brindados, incluyendo el cumplimiento con regulaciones, normas y/o estándares internacionales.
- El proveedor deberá contar con las medidas de protección física necesarias para garantizar que sólo personal autorizado tendrá acceso a los recursos de cómputo, comunicaciones e información reservada.
- El proveedor deberá tener y documentar el proceso utilizado para llevar a cabo la administración de vulnerabilidades, el perfil del personal involucrado, la(s) tecnología(s) utilizada(s) y el alcance del servicio (recomendaciones para el cierre de vulnerabilidades o cierre efectivo de vulnerabilidades). Todo ello con total apego a las disposiciones establecidas en el Manual MAAGTIC-SI.
- El proveedor deberá contar y documentar los controles de seguridad que minimicen el riesgo que representan eventos de software malicioso, como virus, gusanos, troyanos, etc, así como el desarrollo de servicios y productos generados bajo un esquema de seguridad en su ciclo de vida.
- El proveedor deberá contar procedimientos documentados e implementados de Control de Acceso, Registro de Usuarios y Administración de privilegios. Deberá contar con listados de controles de acceso, administración de permisos y privilegios para el resguardo de la información. La administración de control de acceso deberá estar ligada al ciclo de vida de los empleados del proveedor.
- El personal adscrito al posible proveedor deberá tener firmados acuerdos de confidencialidad que cubran tanto los intereses del proveedor como los de sus clientes. Estos acuerdos de confidencialidad deberán ser revisados regularmente – al menos anualmente, a través de un proceso de revisión definido y documentado a petición del IMSS.

La infraestructura ofertada por los posibles proveedores para la partida 1 y 2 deberá ser independiente por cada partida. En caso de que un proveedor resulte ganador en ambas partidas, podrán compartir exclusivamente el servicio de NOC y SOC correspondiente.

Repositorio de información

El posible proveedor deberá incluir en su propuesta técnica un mecanismo de almacenamiento de información <Repositorio> no se requiere compatibilidad con otro repositorio que al menos contenga, a lo largo de la vigencia del contrato, la siguiente información:

- Infraestructura, es decir, el conjunto de componentes habilitadores detallando marca, serie, versión del

sistema operativo o software instalado operando, modelo y principales características (RPV, acceso a Internet, así como herramientas de supervisión, monitoreo y seguridad, NOC y SOC) que formen parte de la solución deberán incluirse en el repositorio.

- Direcciones IP
- Mantenimientos
- Control de Cambios
- Monitoreo (Administración, Continuidad del Negocio)
- Respaldos
- Memoria Técnica detallando los servicios por inmueble, así como diagramas y características de los componentes habilitadores de la solución incluyendo las configuraciones.
- Incidencias
- Facturación
- Ciclo de vida
- Análisis de tendencias
- Plan de mejora de servicios
- Niveles de Servicio
- Tabla de escalación por servicio
- Detalle de la conformación general de la red e infraestructura de telecomunicaciones, así como qué porción es proporcionada por qué empresa del consorcio cuando se trate de participación conjunta.

Además, deberá incluir los entregables de única vez y en caso que sean susceptibles de ser actualizados, deberá incorporar las versiones modificadas durante la vigencia del contrato. También deberá contener el histórico de los entregables periódicos.

El respaldo se refiere a una copia de las configuraciones (versión de sistema operativo, configuración lógica, configuración física) actualizada de todos los CPEs de enrutamiento, seguridad, servicios agregados y equipos activos del servicio. El ciclo de vida se refiere a la fase del proyecto en la que se encuentra cada CPE, equipo activo o terminal (sustitución, operación, etc.).

Respecto a la facturación, solo será requerida aquella información técnica que permite observar la cantidad de servicios utilizados, su costo y aquellos reportes relacionados con el cumplimiento del nivel de servicio.

El repositorio de información deberá permitir acceder a la información mediante consultas a través del protocolo http al menos a 10 usuarios concurrentes que el IMSS designará.

El acceso a dicho repositorio será a través de autenticación proporcionada con login y password al personal designado por el IMSS, permitirá la configuración de roles identificados por usuarios, con el objetivo de mostrar la información de los ID's designados y creación de directorios clasificados por nodo, permitiendo el despliegue individual y privado de la información. La autenticación estaría asociada a otros mecanismos de acceso como LDAP/Directorio Activos, siempre y cuando cumpla con las funcionalidades y niveles de servicio solicitados

Los roles mencionados podrán ser de 3 tipos:

- "Lector", solamente puede ver los documentos publicados
- "Autor", puede ver los documentos publicados y no publicados, añadir documentos, crear o borrar sus propias carpetas; editar, borrar y publicar cualquier documento en el sitio
- "Aprobador", puede ver las carpetas y documentos a los cuales tiene acceso, y puede revisar, aprobar o rechazar documentos

Será responsabilidad del IMSS la administración del sistema de repositorio, aclarando que por administración se entiende altas, bajas y cambios de usuarios, manejo de privilegios, entre otros; y no el mantenimiento y operación de la infraestructura que forme parte de esta solución, mismo que es responsabilidad del proveedor.

La plataforma propuesta por el posible proveedor debe tener las siguientes funcionalidades:

- Control de versiones. La herramienta dará seguimiento de los documentos e impedirá que alguien pueda sobrescribirlos y guardará una versión de cada documento en el que se hayan introducido cambios.
- Perfiles de documentos. La herramienta será capaz de agregar información a los documentos para plantear búsquedas de palabras clave, fechas de modificación o características por ejemplo.
- Publicación de documentos. Los documentos publicados son accesibles para los usuarios del portal en vistas privadas o públicas. Puede especificarse cuándo y cómo se publicarán.
- Suscripciones. Cuando se encuentra información útil en el portal, es posible suscribirse a dicha información para conocer las últimas modificaciones y estar al día de los posibles cambios a que ésta se someta.
- Respaldos periódicos, programables y customizables.

El posible proveedor deberá ofrecer una solución en un solo repositorio, asegurando también que la explotación y acceso a la información será desde una sola herramienta y con capacidad de espacio de almacenamiento de 500 Gbytes como mínimo.

Esta consulta permitirá la exportación o descarga de la información contenida en el repositorio en los formatos nativos de cada una de ellas, conforme a los privilegios establecidos para cada tipo de usuario.

El proveedor deberá de asegurarse que los equipos que operen en el servicio cumplan con un nivel de seguridad que mantenga la información acorde con los estándares y requerimientos que el área de Seguridad Informática del IMSS disponga. La infraestructura para proveer esta funcionalidad estará en las instalaciones del proveedor y siempre y cuando se cumplan las funcionalidades y niveles de servicio solicitados.

El Repositorio de Información, incluyendo la plataforma y la información que en éste reside, pasarán a ser administrados por el IMSS o por quien éste designe, al final del contrato.

8. Condiciones de Continuidad.

Derivado de que el servicio objeto del presente contrato se prestará como continuidad, contados a partir del día siguiente a la notificación de adjudicación y hasta el 31 de diciembre de 2020, con el mismo proveedor que prestaba los servicios desde enero de 2018, para los servicios de enlace de criticidad media y normal, así como para los servicios administrados de acceso a internet, de forma enunciativa más no limitativa no serán aplicables aun cuando así lo mencione el presente Anexo Técnico los siguientes conceptos:

- Las entregas únicas y primigenias previas al inicio de la prestación de los servicios
- El Periodo de habilitación, configuración, transición, pruebas, así como puesta a punto de los servicios objeto del presente Anexo y sus respectivos apéndices
- La entrega de manuales
- La sustitución de equipo de voz, datos o vídeo,
- Los equipos de seguridad perimetral, firewalls,
- La entrega de enlaces de telecomunicaciones ya existentes,
- El manual de la solución propuesta,

- Las topologías, certificaciones de seguridad, políticas, procedimientos y certificados en manejo de seguridad de la información,
- La matriz de escalación del servicio, incluyendo la entrega-recepción de la administración,
- Toda aquella documentación e infraestructura operativa, ya que el proveedor podrá usar toda su base instalada y operativa existente a la fecha.

De la misma manera, por ser un contrato de continuidad de servicios, seguirán teniendo validez los documentos de comprobación administrativa y de descripción del servicio del contrato DC17S0082 y su convenio modificatorio no.1, asimismo quedan sin efecto los niveles de servicio, los periodos estipulados de gracia en la aplicación de penas convencionales y deductivas por concepto de transición de los servicios, ya que se trata de un contrato de continuidad. Los alcances y servicios, así como los niveles de servicio, penas convencionales y deductivas por tratarse de un contrato de continuidad serán las mismas que están estipuladas en el contrato actual DC17S0082 y su convenio modificatorio no.1.

Las condiciones aquí estipuladas prevalecerán en todo momento respecto a lo estipulado en el Anexo Técnico, Apéndices y Términos y Condiciones del presente procedimiento de contratación por lo que en caso de que existiera discrepancia de manera enunciativa más no limitativa en cuanto a los alcances, servicios, entregables y/o niveles de servicio, deductivas, penalizaciones entre otros, lo señalado en el presente numeral será prevalente sobre el presente procedimiento de contratación.

9. Perfil del posible proveedor.

PARTIDA 1

El posible proveedor deberá incluir en su proposición la siguiente documentación:

A. El posible proveedor deberá incluir en su proposición documento en hoja membretada de la empresa en donde indique el personal asignado a los perfiles solicitados por el Instituto, así como la documentación del mismo.
   - o Líder del proyecto: El Instituto requiere 1 (uno). El posible proveedor deberá entregar curriculum profesional en el que acredite que el Líder del Proyecto cuenta con dominio en el servicio solicitado, deberá acreditar 3 (tres) años de experiencia profesional como administrador de proyectos de la misma naturaleza que el objeto del presente procedimiento de contratación o servicios similares, así como 5 (cinco) años de experiencia profesional comprobable en el ramo de telecomunicaciones. El curriculum deberá incluir una descripción detallada de los proyectos en los que ha participado, nombre de la empresa o empresas donde laboró, período en el que laboró y datos del jefe inmediato superior con quien haya laborado. Del mismo modo deberá anexar la documentación académica probatoria referente al nivel licenciatura relacionada con las Tecnologías de Información y Comunicaciones (TIC) concluida y cédula profesional. Deberá entregar también copia simple de la certificación vigente del Project Management Institute como Project Management Professional (PMP) a nombre del Líder del proyecto, en el entendido que dicho certificado deberá estar vigente durante el período que abarque la contratación del servicio.
   - o Coordinadores del servicio: El Instituto requiere 1 (uno) Coordinador del servicio terrestre, 1 (uno) Coordinador del servicio satelital y 1 (uno) Coordinador de centro de monitoreo. En este punto el posible proveedor deberá presentar por cada coordinador el curriculum profesional en el que acredite el domino del servicio a coordinar, el curriculum deberá incluir una descripción detallada de los proyectos en los que ha participado, nombre de la empresa o empresas donde laboró, período en el que laboró y datos del jefe inmediato superior con quien haya laborado. Del mismo modo

deberá entregar la documentación académica probatoria referente al nivel licenciatura relacionada con las Tecnologías de Información y Comunicaciones (TIC) concluida y cédula profesional. Deberá entregar también copia simple de la certificación vigente en ITIL Foundation v3 a nombre del Coordinador del servicio terrestre, Coordinador del servicio satelital y Coordinador del centro de monitoreo, en el entendido que dichos certificados deberán estar vigentes durante el periodo que abarque la contratación del servicio.

- o Personal para soporte a los sitios: En este punto el posible proveedor deberá presentar el curriculum profesional en el que acredite el domino del soporte a los sitios terrestres y satelitales, el curriculum deberá incluir una descripción detallada de los proyectos en los que ha participado, nombre de la empresa o empresas donde laboró, período en el que laboró y datos del jefe inmediato superior con quien haya laborado. Del mismo modo deberá entregar la documentación académica probatoria referente al nivel licenciatura relacionada con las Tecnologías de Información y Comunicaciones (TIC) concluida y cédula profesional, así como copia simple de certificaciones Cisco Certified Network Associate (CCNA) Routing and Switching, a favor de cuando menos cinco de los empleados que prestarán el soporte a los sitios terrestres y satelitales; en el entendido que dichos certificados deberán estar vigentes durante el período que abarque la contratación del servicio.

B. El posible proveedor deberá entregar copia simple del título de concesión vigente por parte de la SCT o de la autoridad competente para enlaces de comunicaciones. El título de concesión deberá contener como mínimo: El nombre y domicilio del concesionario, los servicios que podrá prestar el concesionario y la vigencia del mismo. **No presentar la documentación solicitada en este punto, es causal de desechamiento.**

C. El posible proveedor deberá entregar copia simple del permiso o autorización vigente, expedido por la autoridad correspondiente, con el cual demuestre que se proporcionará el servicio a través de un telepuerto autorizado *(telepuerto instalado y operado en el territorio Nacional)*, o en su defecto copia simple del permiso y/o contrato con el operador autorizado para operar el Telepuerto. **No presentar la documentación solicitada en este punto, es causal de desechamiento.**

D. El posible proveedor deberá entregar copia simple del certificado de homologación de los componentes de la Estación Terrena-Telepuerto, así como copia simple del certificado de homologación de los componentes de la Estación Terrena Remota-VSAT. **No presentar la documentación solicitada en este punto, es causal de desechamiento.**

E. Para lograr tiempos de respuesta óptimos y cumplir con los requerimientos de latencia mínimos solicitados por el Instituto en el anexo técnico, el posible proveedor deberá contar con la conexión directa de su POP de MPLS con el telepuerto de la solución satelital, por lo que deberá entregar la documentación que avale el tipo de conexión y el detalle de ancho de banda.

F. El posible proveedor deberá entregar manifestación escrita firmada por el representante legal de la empresa, en la que indique que el Centro de Monitoreo cumplirá con las especificaciones solicitadas en este anexo técnico, dicha manifestación deberá enlistar cada una de las especificaciones que deberá cumplir el Centro de Monitoreo.

G. El centro de monitoreo deberá ser provisto bajo el entorno de los siguientes estándares internacionales: ISO/IEC 20000-1:2011, ISO 9001:2008 o superior e ISO/IEC 27001:2005. El posible proveedor deberá entregar copia simple de dichas certificaciones, mismas que deberán estar vigentes.

H. El posible proveedor deberá entregar carta en papel membretado y firmada por el representante legal del fabricante de los equipos que integren la solución terrestre y satelital propuesta, en la cual detalle que el posible proveedor es distribuidor autorizado con capacidad de instalar y operar la infraestructura propuesta.

I. El posible proveedor deberá entregar documento en hoja membretada de la empresa la propuesta técnica, mediante la cual acredite que oferta el servicio solicitado en el anexo técnico, mismo que

deberá señalar de manera idéntica al anexo técnico, todas y cada una de las características, requisitos, bienes y servicios solicitados en el mismo, asimismo deberá contener la firma electrónica y/o autógrafa digitalizada del representante legal.

J. El posible proveedor deberá presentar copia simple de contratos debidamente formalizados, el posible proveedor deberá acreditar al menos 1 (uno) año de experiencia en la prestación de servicios iguales o similares al solicitado en el anexo técnico, los servicios descritos en los contratos deberán ser similares al objeto de éste proceso de contratación. Se entenderá por servicio similar aquel que provea de redes terrestres, redes satelitales y centro de monitoreo. Para este punto, el Instituto tomará como válidos a los contratos que en el objeto describan la prestación de alguno de los servicios descritos como similares, es decir, redes terrestres o redes satelitales o centro de monitoreo. Los contratos deberán haber sido celebrados con empresas, dependencias y/o entidades de la administración pública federal, no podrán tener fecha de firma anterior al año 2010 y no podrán tener una vigencia menor a 1(uno) año, se aceptará la presentación de contratos plurianuales. El posible proveedor deberá resaltar en los contratos: la vigencia, el número de contrato, objeto del contrato, resumen de servicios incluidos y cliente o beneficiario de los mismos. Asimismo el posible proveedor deberá anexar los nombres, correo electrónico y teléfonos del personal de contacto con los clientes de dicho contrato para efectos de verificación de la información proporcionada.

K. El posible proveedor deberá presentar copia simple de contratos debidamente formalizados, el posible proveedor deberá acreditar especialidad en la prestación de servicios similares al solicitado en el anexo técnico, los servicios descritos en los contratos deberán ser similares al objeto de éste proceso de contratación. Se entenderá por servicio similar aquel que provea de redes terrestres, redes satelitales y centro de monitoreo. Para este punto, el Instituto tomará como válidos a los contratos que en su objeto describan la prestación de los tres servicios descritos como similares, es decir, redes terrestres y redes satelitales y centro de monitoreo. Los contratos deberán haber sido celebrados con empresas, dependencias y/o entidades de la administración pública federal, no podrán tener fecha de firma anterior al año 2010 y no podrán tener una vigencia menor a 1 (uno) año, se aceptará la presentación de contratos plurianuales. El posible proveedor deberá resaltar en los contratos: la vigencia, el número de contrato, objeto del contrato, resumen de servicios incluidos y cliente o beneficiario de los mismos. Asimismo, el posible proveedor deberá anexar los nombres, correo electrónico y teléfonos del personal de contacto con los clientes de dicho contrato para efectos de verificación de la información proporcionada.

L. El posible proveedor deberá incluir en su proposición documento en hoja membretada de la empresa en el que indique la metodología, procesos y procedimientos que utilizará para prestar el servicio solicitado, éste documento deberá indicar la forma en la que el posible proveedor logrará técnicamente entregar el servicio a solicitado, el modelo que utilizará para el manejo de los diferentes perfiles que intervienen en sus procesos, la organización de su mesa de servicios, el proceso de atención a incidentes, así como la metodología, formatos y procedimientos que utilizará para medir en forma mensual la satisfacción del servicio que recibe el Instituto y las estrategias que llevará a cabo para lograr un proceso de mejora continua. No se aceptarán cartas bajo protesta de decir verdad en las que se comprometa el cumplimiento de cualquiera de las especificaciones del servicio.

M. El posible proveedor deberá incluir en su proposición documento en hoja membretada de la empresa en el que indique el modelo de matriz de escalación que utilizará para controlar el servicio que proporcionará al Instituto durante la vigencia del contrato, asimismo, la matriz de escalación deberá describir los tiempos definidos para la atención y solución a fallas en el servicio, incluyendo los medios de contacto electrónico, tales como correo electrónico y teléfonos tanto fijos como celulares.

N. El posible proveedor deberá incluir en su proposición en hoja membretada de la empresa la plantilla de los recursos humanos con los que cuenta para la prestación del servicio solicitado.

O. El posible proveedor deberá presentar copia simple de al menos 1 (uno) contrato de servicios similares al solicitado en el anexo técnico, se entenderá por servicio similar aquel que provea de redes terrestres, redes satelitales y centro de monitoreo. Los contratos deberán haber sido celebrados con empresas, dependencias y/o entidades de la administración pública federal, no podrán tener fecha de firma anterior al año 2010 y no podrán tener una vigencia menor a 1 (uno) año, se aceptará la presentación de contratos plurianuales. Los contratos deberán estar acompañados del documento que haga constar la cancelación de la garantía de cumplimiento respectiva, manifestación expresa de la contratante sobre el cumplimiento total de las obligaciones a cargo del posible proveedor o cualquier otro documento con el que se corrobore dicho cumplimiento, el contrato deberá estar debidamente concluido. En caso de presentar manifestación o cualquier otro documento con el que se corrobore el cumplimiento, deberá incluir el nombre, cargo, teléfono, correo electrónico, correo y rol del respectivo contrato, los servicios descritos en los contratos deberán ser similares al objeto de éste proceso de contratación, se entenderá por servicio similar aquel que provea de redes terrestres, redes satelitales, centro de monitoreo. El posible proveedor deberá resaltar en los contratos: la vigencia, el número de contrato, objeto del contrato, resumen de servicios incluidos y cliente o beneficiario de los mismos. Asimismo, el posible proveedor deberá anexar los nombres, correo electrónico y teléfonos del personal de contacto con los clientes de dicho contrato para efectos de verificación de la información proporcionada.

PARTIDA 2

El posible proveedor deberá incluir en su proposición la siguiente documentación:

No.	Descripción
1	Aceptación de la totalidad de los capítulos y secciones contenidos en este anexo técnico, para lo cual el posible proveedor debe emplear el mismo orden y secuencia de temas que comprende este 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 para evitar ambigüedades en la suscripción.
2	Descripción a alto nivel de la arquitectura global que el posible proveedor utilizará para prestar los servicios objeto de este anexo técnico, apegándose a la Arquitectura de Referencia definida en éste. Este documento debe describir de forma general, las características de los componentes necesarios para entregar cada uno de los servicios administrados, pudiendo apoyarse para consolidar un documento concreto y conciso, en esquemas, diagramas, tablas, listados o cualquier elemento didáctico que el posible proveedor 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.
3	Descripción de la metodología, procesos, procedimientos y alianzas que el posible proveedor utilizará para la prestación de los servicios a contratar. Este documento hablará de la forma en la que el posible proveedor consolidará los diversos servicios, funcionalidades y tareas solicitadas en este Anexo Técnico a partir de sus métodos, mejores prácticas, alianzas comerciales y demás mecanismos de entrega de servicio.
4	Relación y descripción detallada de todos los Componentes Habilitadores, red de telecomunicaciones e Infraestructura Auxiliar que formarán parte de su solución para proveer los servicios descritos en el presente documento, en cualquiera de los elementos del Catálogo de Servicios correspondiente, conforme a lo establecido en este documento, que describan las características y especificaciones técnicas del fabricante de cada uno de ellos, para los casos en los que esto aplique. Las funcionalidades de estos servicios no deben ser referenciados a un catálogo de fabricante, no obstante, de conformidad a lo establecido en el anexo técnico, deberá incluirlos y detallarlos.

5	Descripción detallada de cómo logrará el posible proveedor técnicamente, entregar los Servicios Administrados de Acceso a Internet, de acuerdo a cada uno de las secciones comprendidas en el anexo técnico. Para construir este documento, el posible proveedor puede utilizar esquemas, descripciones de equipo y de software, métodos de integración de aplicaciones y hardware y cualquier elemento didáctico que considere conveniente para lograr una descripción lógica, comprensible y detallada de todos los Componentes Habilitadores, red de telecomunicaciones e Infraestructura Auxiliar.
6	Descripción detallada de cómo logrará el posible proveedor técnicamente, entregar todos y cada uno de los Servicios Operativos, de acuerdo a cada una de las secciones comprendidas en la sección del mismo nombre en el Anexo Técnico. Para construir este documento, el posible proveedor puede utilizar esquemas, descripciones de equipo y de software, métodos de integración de aplicaciones y hardware y cualquier elemento didáctico que considere conveniente para lograr una descripción lógica, comprensible y detallada.
7	Descripción del programa de Mantenimientos y Correctivos, y de los procedimientos, técnicas, prácticas y consideraciones que el posible proveedor ofrecerá para cubrir dichos servicios, de acuerdo a los Niveles de Servicio especificados en el presente documento. Deberá incluir, al menos: · La descripción de los procesos asociados a la labor · Los Recursos Humanos y Materiales involucrados · El tiempo definido para la atención de requerimientos y/o solución de fallas o los compromisos de acuerdo a los niveles de servicio solicitados en este documento · Los alcances técnicos del mantenimiento y los protocolos de prueba · Las rutas de escalamiento correspondientes
8	Descripción clara de cómo el proveedor proporcionará los Procesos de Administración de Problemas y los servicios de SOC, incluyendo las consideraciones técnicas de diseño, procedimientos y operación correspondientes, de acuerdo a lo especificado en las secciones dedicadas a estas solicitudes en el Anexo Técnico.
9	Manifestación escrita firmada por el Representante Legal de la empresa, en la que establezca que cuenta con las garantías y el soporte de los fabricantes de los Componentes Habilitadores de hardware y software, así como de los diferentes elementos de infraestructura auxiliar que incluya y que formen parte de la solución de los Servicios Administrados de Acceso a Internet, y que cuenta con personal calificado para efectuar el diseño, análisis, evaluación, operación, administración y mantenimiento de todos los servicios soportados por dichos Componentes Habilitadores y elementos activos.
10	Manifestación escrita firmada por el Representante Legal de la empresa, en la que establezca que cuenta con el personal calificado y debidamente certificado al más alto nivel por parte del fabricante de la solución tecnológica propuesta sobre los diferentes componentes activos (deberá explícitamente abundar sobre: equipo CPE de Internet, clean pipes, componentes habilitadores y soluciones de seguridad, SOC) que formen parte de su solución para conducir las tareas de instalación, puesta en marcha, configuración, soporte, monitoreo y operación de los servicios objeto de este anexo técnico.
11	Manifestación escrita firmada por el Representante Legal de la empresa, en la que ésta garantice específicamente la calidad de los trabajos y de los materiales menores a emplear en la instalación, a efectos de no presentar estos vicios ocultos al menos en la vigencia del contrato.
12	Manifestación escrita firmada por el Representante Legal de la empresa, en la que establezca con claridad que los equipos suministrados cuentan con las garantías solicitadas por parte de los fabricantes o distribuidores autorizados de los principales Componentes Habilitadores de Hardware y Software que integre a su solución.

13	Organigrama y currículo del personal inicial que será encargado de proporcionar el servicio contratado, de cara al IMSS. El posible proveedor deberá incluir hasta tres niveles (1-2-3) en el detalle top-bottom del organigrama, con la información requerida. Deberá anexar a este entregable de su Propuesta Técnica, todos los currículos del personal de soporte certificado solicitado de manera obligatoria como parte de este Anexo Técnico, indicando las certificaciones con las que cuenta y la fecha de obtención y caducidad del certificado en cuestión.
14	El posible proveedor dará cumplimiento a los niveles de servicio solicitados en el anexo técnico, para lo cual deberá suscribir como parte de su propuesta, las tablas con las métricas de nivel de servicio referidas, manifestando el compromiso explícito de dar cumplimiento a las mismas.
15	Entrega de documentos probatorios de experiencia, capacidades, habilidades y certificaciones del personal a cargo de los procesos del SOC, mediante la siguiente información: Copias de certificados vigentes, currículos actualizados, así como copia de las certificaciones solicitadas.
16	Manifestación escrita firmada por el representante legal de la empresa, donde exprese que dicha empresa cuenta con un DRP (Disaster Recovery Plan, por sus siglas en inglés) para el respaldo de información crítica para la operación de los servicios. A la manifestación escrita, deberá acompañar un documento técnico donde se explique dicho plan y cómo se vincula con los servicios específicos objeto de esta contratación.
17	Manifestación escrita, firmada por el representante legal de la empresa en el que manifieste que cuenta con al menos 5 años de experiencia en la provisión de servicios de SOC como los solicitados en esta contratación. El objetivo del requisito es demostrar al IMSS al menos cinco años de experiencia en proyectos relacionados con seguridad de información, para lo cual podrá acompañar copia simple de al menos un contrato que satisfaga la cantidad de tiempo expresada, junto con un resumen de éste, en el que se manifieste dicha experiencia de forma explícita.
18	Manifestación escrita firmada por el representante legal de la compañía, que indique que ésta cuenta con personal con certificación vigente en "ITIL Versión 3, nivel Expert y que la provisión y operación de los servicios objeto de esta contratación será debidamente realizada y supervisada por el personal que cuente con dicha certificación durante la vigencia del contrato (demostrando esta condición al menos para un recurso humano vinculado al servicio del IMSS). El posible proveedor deberá incluir de manera obligatoria, copia(s) de la(s) certificación(es), emitida por un organismo autorizado para realizar dicha certificación, donde pueda validarse a través de un número la vigencia de dicha certificación.
19	Manifestación escrita, firmada por el representante legal de la empresa en la cual especifica que cuenta con las alianzas necesarias con los fabricantes de las soluciones necesarias para el otorgamiento de los Servicios Administrados objeto de este anexo técnico. **No presentar la documentación solicitada en este punto, es causal de desechamiento.**
20	Manifestación escrita firmada por el representante legal de la empresa, donde indique que cuenta con un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) que cumplan con los requisitos solicitados por el IMSS en este anexo técnico. Deberá de adjuntar a dicha carta, un documento integral que con mucho detalle especifique la ubicación, procesos, certificaciones e infraestructura de dicho Centro de Operaciones de Seguridad.
21	Documento de propuesta del proceso de atención de problemas, alineada a las mejores prácticas establecidas en ITIL. Dicha propuesta deberá contar, al menos, con los siguientes elementos: Clasificación de tipo de falla, tiempo de respuesta por tipo de falla, proceso de atención a falla, tiempo de resolución de falla.
22	Las áreas que brindarán el servicio de SOC al IMSS deberán estar certificadas en ISO/IEC 27001:2005. El posible proveedor deberá entregar copia del documento de certificación que permita al IMSS vincular dicho proceso con el servicio solicitado en este anexo técnico y además, deberá presentar una manifestación escrita firmada por el representante legal de la empresa en el que asegure contar con

	dicha certificación, anexando el documento probatorio, la entidad certificadora y su vigencia.
23	Manifestación por escrito, firmada por el representante legal de la empresa, 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.
24	Manifestación por escrito firmada por el representante legal de la empresa, en la que expresa que el personal encargado del diseño de la arquitectura de la solución tecnológica propuesta por los posibles proveedores acredita la certificación en PMI (certificado profesional en dirección de proyectos emitido por el Project Management Institute) o TOGAF (certificado en la Metodología y Herramientas para Desarrolar Arquitecturas en Empresas), incluyendo copia de la acreditación correspondiente.
25	Manifestación escrita, firmada por el representante legal del licitante, en la que indique que su representada cuenta en su plantilla de personal con al menos cinco trabajadores con estudios a nivel licenciatura en carreras afines o relacionadas con la operación y administración de tecnologías de la información y comunicaciones. para la acreditación de este requisito deberán presentar las cédulas profesionales correspondientes certificadas por un notario público.
26	Manifestación escrita firmada por el Representante Legal de la empresa en la cual especifica que cuenta con las alianzas necesarias con los fabricantes de las soluciones necesarias para el otorgamiento de los servicios administrados objeto de este anexo técnico. **No presentar la documentación solicitada en este punto, es causal de desechamiento.**

10.Condiciones técnicas de aceptación de los entregables.

PARTIDA 1

El proveedor está obligado a proporcionar el servicio solicitado a todos los sitios señalados en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual".

Para hacer constar que la prestación del servicio se llevó a cabo a entera satisfacción del Instituto, el proveedor deberá elaborar:

- Sitios terrestres: Protocolo de Pruebas para la Entrega de Sitios Terrestres Tipo A, (Apéndice 4).
- Sitios satelitales: Protocolo de Pruebas para la Entrega de Sitios Satelitales Tipo B, (Apéndice 5).

Ambos documentos se adjuntan al presente anexo y deberán ser entregados al Administrador del Contrato debidamente requisitados y firmados por el proveedor y por el Instituto.

PARTIDA 2

Entregables por Única Vez

El proveedor se compromete a entregar, de manera única a lo largo de la vigencia del contrato, un conjunto de documentos relacionados con su servicio. A continuación, se puntualizan los entregables mínimos para su mejor atención.

NÚMERO	NOMBRE Y DESCRIPCIÓN	LÍMITE DE ENTREGA
1	Matriz de Escalación	5 días naturales posteriores a la finalización de mesas de trabajo

2	Procedimiento de Control de Cambios	5 días naturales posteriores a la finalización de mesas de trabajo
3	Escrito del posible proveedor sobre las capacidades y habilidades para soportar los equipos.	45 días naturales posteriores a la notificación del fallo
4	Aseguramiento de Calidad en la Entrega	30 días naturales posteriores a la entrega del inmueble
5	Plan de trabajo nuevos inmuebles o reubicaciones	5 días naturales posteriores a la solicitud de cambio de inmueble o reubicaciones
6	Checklist de liberación del inmueble	5 días naturales posteriores a la migración del inmueble
7	Memorias Técnicas	10 días naturales posteriores a la entrega del inmueble
8	Procedimiento en caso de contingencia (Continuidad del Negocio)	30 días naturales posteriores a la firma del contrato
9	Plan de trabajo de transición de los servicios	2 meses antes de la finalización del contrato
10	Documentación generada en fase de migración	45 días naturales posteriores a la entrega del último inmueble
11	Categorizaciones para Mesa de Ayuda del IMSS	5 días naturales posteriores a la finalización de mesas de trabajo

Entregables Periódicos

A continuación, y como complemento a lo establecido en la sección anterior, se puntualizan aquellos entregables obligatorios bajo el criterio de entrega periódica, que serán elaborados y entregados al IMSS por el proveedor:

NÚMERO	NOMBRE Y DESCRIPCIÓN	FRECUENCIA DEL REPORTE
1	El proveedor entregará reportes de administración de configuraciones y cambios en la infraestructura, así como la actualización de una memoria técnica integral de los servicios.	Cada tres meses o cada vez que se efectúen cambios por alta, baja y cambio de nodo de la RPV
2	Disponibilidad, Latencia y Degradación por Pérdida de Paquetes, por sitio y por elemento funcional que forme parte de la solución. La información contenida será real sin sumarización o compactación, así como ser posible, para cada clase de servicio conforme a lo establecido anteriormente.	Se entregarán dentro de los primeros 5 días hábiles de cada mes
3.	Reporte de Atención y solución de fallas. Indicando los tipos de fallas, su tiempo medio de reparación (MTTR), si afectan o no la disponibilidad	Se entregarán dentro de los primeros 5 días hábiles de cada mes
4.	Disponibilidad, Latencia y Degradación por Pérdida de Paquetes del acceso a Internet, por sitio. La información contenida será real sin sumarización o compactación.	Se entregarán dentro de los primeros 5 días hábiles de cada mes
5.	Reporte ejecutivo. Contendrá estadísticas principales de uso y desempeño de todos los nodos.	Se entregará de manera anual, por periodos de 6 meses
6	Informes Ejecutivos por incidente. Este informe ejecutivo contendrá la descripción sencilla de la falla, sus causas y las acciones que se tomaron para	El proveedor entregará a solicitud del IMSS, un reporte ejecutivo de los incidentes que considere críticos

NÚMERO	NOMBRE Y DESCRIPCIÓN	FRECUENCIA DEL REPORTE
	resolverlas, el formato y la forma de entrega se definirá con el proveedor como parte de las reglas de operación. Sin embargo, el formato será electrónico.	
7	Informes de gestión del SOC	Se entregarán dentro de los primeros 5 días hábiles de cada mes

Reportes en Línea

El proveedor deberá tener disponibles, a lo largo de la vigencia del contrato, un conjunto de reportes en línea, mismos que puedan ser revisados por los funcionarios responsables del gobierno del servicio al interior del IMSS. A continuación, se puntualizan los entregables mínimos para su mejor atención. Se acordará en las Mesas de trabajo un tiempo con el posible proveedor que resulte adjudicado, para poder adecuar la herramienta a sus necesidades específicas.

Tipo de Reporte	Descripción	Formato	Periodos
a) Reporte de salud	Muestra la salud de la red o grupo de elementos basados en la utilización y errores detectados. Permite verificar el desempeño actual e histórico de los elementos o grupos de elementos. Ver subreportes en seguida: Reportes de Excepciones. Reportes Resumidos Reportes -Top Ten Reportes Detallados por Elemento Reportes Suplementarios.	HTML, PDF, ASCII	Diario Semanal Mensual
a.1) Reporte de salud: Excepciones	Permite determinar si un elemento en particular experimenta altos volúmenes, errores o errores repentinos Detalla la causa principal y despliega la tendencia de la condición; enlista las excepciones por prioridad.		
a.2) Reporte de salud: Resumen	Describe un resumen del rendimiento de los servicios utilizando cuatro gráficas: volumen total (sea en meses, semanas o días, anexando tablas de valores), volumen promedio, índice de salud promedio y situaciones a observar. Permite conocer tendencias y patrones regulares de tráfico en el tiempo.		
a.3) Reporte de salud: Top Ten	Muestra los enlaces más ocupados en la red administrada, basados en el volumen o índice de salud, así como los líderes en cambio tanto en volumen como en índice de salud.		
a.4) Reporte de salud Detallados por Elemento	Permite verificar el desempeño de cada circuito en la red. Ofrece comparativos de volumen contra la línea de base (4 semanas) o promedio histórico. Presenta el grado de ocupación de elementos por categorías mostradas en colores.		
b) Reporte detallado a la demanda	Muestra el rendimiento de los servicios durante un periodo de tiempo determinado, tomando en cuenta utilización de ancho de banda, bytes, frames, descartes, errores, disponibilidad, latencia y alcanzabilidad.	HTML, PDF, ASCII	Diario
c) Reporte de tendencias	Permite analizar el rendimiento de un servicio o conjunto de servicios sobre una variable (uso de ancho de banda, utilización de ancho de banda en horarios de operación de los inmuebles por ejemplo); así como identificar la causa de alguna degradación del rendimiento.	HTML, PDF, ASCII	Diario
d) Reporte de	Reportado por medio de Cisco Network Based Application	HTML,	

Tipo de Reporte	Descripción	Formato	Periodos
desglose de tráfico por protocolo en enlaces WAN	Recognition (Cisco NBAR), presenta el desglose de protocolos que cursan sobre el enlace durante el periodo solicitado. El posible proveedor deberá integrar en su proposición cualquier herramienta para el reporte de tráfico por protocolo en enlaces WAN que cubra las características solicitadas, así como la funcionalidad y niveles de servicio solicitados.	PDF, ASCII	Diario
e) Monitoreo de niveles de servicio (SLA)	Herramienta para revisar en línea la disponibilidad del nodo y el retardo en los enlaces (Round Trip Time Delay). Capacidad de consultar de manera inmediata reportes de los 10 nodos con máximo RTT; disponibilidad promedio de los enlaces WAN y distribución de las disponibilidades de la red en categorías por colores.	HTML, PDF, ASCII	Diario

11. Cronograma de actividades

PARTIDA 1

ACTIVIDAD	MES					
	DURACIÓN	1	2	3	4	5
Mesas de trabajo para la continuidad del servicio.	7 días					
Entrega de certificados para el centro de monitoreo por parte del proveedor.	7 días					
Validación de operaciones del centro de monitoreo con el Instituto.	7 días					
Firma de Acuerdos de Nivel de Operación (OLAs) entre el Proveedor y los Terceros Involucrados con vigilancia del Grupo Administrador del Contrato del IMSS	7 días					
Prestación del servicio efectivo por parte del proveedor.	5 meses					

El Instituto brindará al proveedor un directorio general actualizado para brindar el soporte con los usuarios de sitio y/o coordinar visitas de servicio, el directorio contendrá: nombre del sitio, responsable de sitio, número telefónico de contacto, y correo electrónico del responsable.

PARTIDA 2

ID	HITO	MES					
		DURACION	1	2	3	4	5
1	Mesas de trabajo para la continuidad del servicio.	7 días					
2	Firma de Acuerdos de Nivel de Operación (OLAs) entre el Proveedor y los Terceros Involucrados con vigilancia del Administrador del Contrato del IMSS	7 días					
3	Inicio de los Trabajos de Preparación para el Nuevo Servicio	A más tardar 3 meses antes del día de la Finalización del Contrato					
4	Prestación del servicio efectivo por parte del proveedor.	5 meses					

12. Niveles de servicio acordados que deberán cumplirse

PARTIDA 1

Servicio Administrado de Red Privada Virtual.

No.	SERVICIO	NIVEL
1	DISPONIBILIDAD DE ENLACES TERRESTRES.	98.89%
2	DISPONIBILIDAD DE ENLACES SATELITALES.	98.89%
3	DISPONIBILIDAD DE MESA DE SERVICIOS.	7X24X365

El porcentaje de disponibilidad está expresado en promedio mensual.

PARTIDA 2

Servicio Administrado de Acceso a Internet.

Tipo de Nivel de Servicio	Descripción de Nivel de Servicio	Métrica Objetivo Mensual
Disponibilidad	Disponibilidad de los Servicios Administrados de Acceso a Internet (por Nodo)	99.98%
Disponibilidad	Disponibilidad del Servicio de Prevención de Intrusos (IPS)	99.96%
Disponibilidad	Disponibilidad del Servicio de Firewall en Alta Disponibilidad	99.96%
Disponibilidad	Disponibilidad del Servicio de Análisis de Flujo	99.96%
Disponibilidad	Disponibilidad del Servicio de Control de Acceso a Páginas Web	99.96%
Disponibilidad	Disponibilidad del Servicio de Análisis de Vulnerabilidades	99.96%
Disponibilidad	Disponibilidad del Servicio de Proxy	99.96%
Entrega	Entrega de modificaciones en Ancho de Banda de Internet	95% de las veces en 4 horas o menos
Desempeño	Latencia	Menor a 100 milisegundos de ida y vuelta al Punto de Acceso a la Red más cercano

13. Requerimientos de arquitectura tecnológica

El servicio deberá integrar la interconexión con el Sitio Nube IMSS Digital (también conocido como Punto Neutro), ubicado en Santa Fe, con la red MPLS, en la que se integran los enlaces de los sitios señalados en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual"; así como en los sitios que el Instituto designe, para lo cual el posible proveedor deberá utilizar los enlaces con capacidad de 200 Mbps de forma sumarizada.

El posible proveedor deberá suministrar los equipos de ruteo requeridos para soportar la interconexión solicitada en el párrafo anterior, así como los servicios de configuración y puesta a punto de la mencionada interconexión.

14. Restricciones e interfaces con otros elementos

No aplica

15. Causales de desechamiento.

Deberá referirse al incumplimiento de los puntos las señaladas en el numeral 6. Perfil del posible proveedor del presente anexo técnico.

16. Formato de declaración de no conflicto de interés.

Con base en lo indicado en las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto, punto 4 Políticas, apartado 4.15, inciso i, se anexa al presente el Anexo 4, Declaración de no conflicto de interés.

17. Firmas de elaboración, revisión y aprobación

Responsable de Elaboración

ING. JOSÉ CARLOS ARAGÓN HERRERA
ENCARGADO DEL DESPACHO DE LA DIVISIÓN DE TELECOMUNICACIONES DE CONFORMIDAD CON EL OFICIO NO. 09 52 76 61 5300/202000121, DE FECHA 28 DE FEBRERO DE 2020.

Responsable de Revisión

ING. HUGO OLVERA ORTEGA
COORDINADOR TÉCNICO DE REDES Y TELECOMUNICACIONES

Responsable de Aprobación

ING. EDUARDO OROPEZA ORTIZ
TITULAR DE LA COORDINACIÓN DE SISTEMAS DE INFRAESTRUCTURA TECNOLÓGICA INSTITUCIONAL

18. Relación de Anexos

Id.	Nombre	Descripción corta	Fecha de integración al producto
SGMP TRA 01	Apéndice 1	Inventario de Nodos para el Servicio Administrado de Red Privada Virtual.	20/05/2020
SGMP TRA 02	Apéndice 2	Inventario de Nodos para el Servicio Administrado de Acceso a Internet.	20/05/2020
SGMP TRA 03	Apéndice 3	Cobertura de la Red de Telecomunicaciones del posible proveedor para los Enlaces de Internet	20/05/2020
SGMP TRA 04	Apéndice 4	Protocolo de Pruebas para la Entrega de Sitios	20/05/2020

Id.	Nombre	Descripción corta	Fecha de integración al producto
		Terrestres "Tipo A"	
SGMP TRA 05	Apéndice 5	Protocolo de Pruebas para la Entrega de Sitios Satelitales "Tipo B"	20/05/2020
SGMP TRA 06	Apéndice 6	Declaración de no conflicto de interés	20/05/2020
SGMP TRA 07	TC	Términos y Condiciones	20/05/2020

ANEXOS

DIVISÍON DE CONTRATOS

SIN TEXTO

APÉNDICE 2: Inventario de Nodos para el Servicio Administrado de Acceso a Internet

ID DE INMUEBLE	NOMBRE DEL INMUEBLE	UBICACIÓN: LATITUD_N	UBICACIÓN: LONGITUD_D	DOMICILIO	LOCALIDAD O COLONIA	MUNICIPIO	ESTADO	CÓDIGO POSTAL	HORARIO HÁBIL DEL INMUEBLE	ANCHO DE BANDA "PISO" (Mbps)	ANCHO DE BANDA "TECHO" (Mbps)
70092	CENTRO DE DATOS "NUBE IMSS DIGITAL"	19.363597	-99.28043	Prolongación Paseo de la Reforma 5396, Col. Cuajimalpa, D.F., 05100	CUAJIMALPA	CUAJIMALPA	DISTRITO FEDERAL	05100	7X24X365	300	1000
70089	CENTRO DE DATOS CENATI DF	19.42332778	-99.17266667	TOKIO 80, P. B., COL. JUAREZ, 06600 MEXICO, D.F.	JUÁREZ	CUAUHTÉMOC	DISTRITO FEDERAL	06600	7X24X365	32	155
70090	CENTRO DE DATOS CENATI MONTERREY	25.6715861	-100.298117	GREGORIO TORRES QUEVEDO 1950, ENTRE FELIX U. GOMEZ Y PROF. G. TORRES	ZONA CENTRO	MONTERREY N.L.	NUEVO LEON	64010	7X24X365	155	1000

ANEXOS

DIVISÍON DE CONTRATOS

SIN TEXTO

APÉNDICE 3: Cobertura de la Red de Telecomunicaciones del posible proveedor para los Enlaces de Internet

										opciones aceptables: si / no	opciones aceptables: Propiedad / propio / no tiene	Dirección del POP	Formato equiparable a la columna "C"	formato equiparable a la columna "D"	Distancia expresada en km	fibra óptica
ID DE INMUEBLE	NOMBRE DEL INMUEBLE	UBICACIÓN: LATITUD_N	UBICACIÓN: LONGITUD_O	DOMICILIO	LOCALIDAD O COLONIA	MUNICIPIO	ESTADO	CÓDIGO POSTAL	HORARIO HÁBIL DEL INMUEBLE	El Licitante tiene un Pop para Atender el Inmueble	El PoP referido en la columna H es propiedad del Licitante	Ubicación del PoP referido en la columna H	UBICACIÓN: LATITUD_C2 del POP referido en la columna H	UBICACIÓN: LONGITUD_C3 del POP referido en la columna H	Distancia del PoP de la columna H al Inmueble	Medio de Transmisión del PoP al Inmueble
70092	CENTRO DE DATOS "NUBE IMSS DIGITAL"	19.363597	99.28063	Prolongación Paseo de la Reforma 5396, Col. Cuajimalpa, D.F., 05100	CUAJIMALPA	CUAJIMALPA	DISTRITO FEDERAL	05100	7X24X365							
70089	CENTRO DE DATOS CENATI DF	19.42332778	99.12766667	TOKIO 30, P. B., COL. JUAREZ, C.P.06600 MEXICO, D.F.	JUÁREZ	CUAUHTÉMOC	DISTRITO FEDERAL	06600	7X24X365							
70090	CENTRO DE DATOS CENATI MONTERREY	25.6715861	-100.258117	GREGORIO TORRES QUEVEDO 1950, ENTRE FELIX U. GOMEZ Y PROF. G. TORRES	ZONA CENTRO	MONTERREY	NUEVO LEON	64010	7X24X365							

ANEXOS

DIVISIÓN DE CONTRATOS

SIN TEXTO

Protocolo de Pruebas para la Entrega de Sitios Terrestres, Tipo "A"

Fecha: _____
Número de ID: _____
Nombre del Sitio: _____
Tipo de Movimiento: _____
Domicilio: _____
Ancho de Banda: _____
Router (marca, modelo): _____
Router (número de parte/serie): _____
UPS (Marca, Modelo, Serie): _____
Equipo Adicional (Cantidad y Modelo): _____

Prueba			Método	Satisfactorio (SI / NO)	Observaciones
1	Transmisión y recepción de información	Conectividad entre el Sitio de Prueba y el Sitio Central (Nube IMSS Digital)	Realizar prueba de ping y/o trace route, a una dirección IP válida (p.e. default gateway) en el sitio Nube IMSS Digital proporcionada por el área técnica del IMSS		
2	Transmisión y recepción de información	Conectividad entre el Sitio de Prueba y otro sitio remoto.	Realizar prueba de ping y/o trace route, a una dirección IP válida del sitio remoto proporcionada por el área técnica del IMSS		

Consideraciones para las pruebas:

1. Las pruebas se realizarán bajo responsabilidad mutua entre el personal del IMSS en sitio y el ingeniero del licitante.
2. En caso de que el personal del IMSS no tenga el equipo necesario para realizar la prueba, el ingeniero del licitante deberá de realizarla con su equipo laptop, conectando directamente al puerto ethernet del modem satelital.
3. En caso de que haya problemas de alcanzabilidad con el equipo proporcionado por el IMSS, el ingeniero del licitante deberá de realizar la prueba con su equipo laptop, conectando directamente al puerto ethernet del modem satelital con el fin de delimitar el error de la prueba.
4. Cualquier desviación a las pruebas deberá documentarse en la parte de comentarios o anexar la documentación necesaria.
5. Deberá llenar el protocolo completo con la ayuda del personal del IMSS, el cual firmará el documento como validación de las pruebas y servicio.

Nombre y firma del ingeniero del Licitante

Nombre y firma del personal del IMSS

SIN TEXTO

Protocolo de Pruebas para la Entrega de Sitios Satelitales, Tipo "B"

Fecha: _____
Número de ID: _____
Nombre del Sitio: _____
Tipo de Movimiento: _____
Domicilio: _____
Ancho de Banda: _____
Modem Satelital (Marca, Modelo, Serie): _____
UPS (Marca, Modelo, Serie): _____
Equipo Adicional (Cantidad y Modelo): _____

Prueba			Método	Satisfactorio (SI / NO)	Observaciones
1	Transmisión y recepción de información	Conectividad entre el Sitio de Prueba y el Sitio Central (Nube IMSS Digital)	Realizar prueba de ping y/o trace route, a una dirección IP válida (p.e. default gateway) en el sitio Nube IMSS Digital proporcionada por el área técnica del IMSS		
2	Transmisión y recepción de información	Conectividad entre el Sitio de Prueba y otro sitio remoto.	Realizar prueba de ping y/o trace route, a una dirección IP válida del sitio remoto proporcionada por el área técnica del IMSS		

Consideraciones para las pruebas:

1. Las pruebas se realizarán bajo responsabilidad mutua entre el personal del IMSS en sitio y el ingeniero del licitante.
2. En caso de que el personal del IMSS no tenga el equipo necesario para realizar la prueba, el ingeniero del licitante deberá de realizarla con su equipo laptop, conectando directamente al puerto ethernet del modem satelital.
3. En caso de que haya problemas de alcanzabilidad con el equipo proporcionado por el IMSS, el ingeniero del licitante deberá de realizar la prueba con su equipo laptop, conectando directamente al puerto ethernet del modem satelital con el fin de delimitar el error de la prueba.
4. Cualquier desviación a las pruebas deberá documentarse en la parte de comentarios o anexar la documentación necesaria.
5. Deberá llenar el protocolo completo con la ayuda del personal del IMSS, el cual firmará el documento como validación de las pruebas y servicio.

_____ Nombre y firma del ingeniero del Licitante

_____ Nombre y firma del personal del IMSS

SIN TEXTO

INSTITUTO MEXICANO DEL SEGURO SOCIAL

DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

SERVICIO DE COMUNICACIÓN PARA ENLACES DE CRITICIDAD MEDIA Y NORMAL DEL IMSS

TÉRMINOS Y CONDICIONES

2020

ANEXOS

DIVISÍON DE CONTRATOS

Contenido

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
Ver. 1.0	18/03/2020	Documento inicial	Ing. José Carlos Aragón Herrera
Ver. 1.1	17/04/2020	Actualización del documento	Ing. José Carlos Aragón Herrera
Ver. 1.5	20/05/2020	Actualización del documento	Ing. José Carlos Aragón Herrera
Ver. 1.6	29/05/2020	Aprobación del documento	Ing. Eduardo Oropeza Ortiz

ANEXOS
DIVISIÓN DE CONTRATOS

1. Objetivo del documento.

El objetivo del presente documento es establecer los términos y condiciones mínimos necesarios que el proveedor debe cumplir para otorgar el "Servicio de comunicación para enlaces de criticidad media y normal del IMSS", en lo sucesivo el servicio.

2. Administrador del Contrato y Área Técnica.

El Administrador del Contrato será el Titular Coordinación de Sistemas de Infraestructura Institucional y el Área Técnica estará conformado por el por el Titular de la Coordinación Técnica de Redes y Telecomunicaciones y por el Titular de la División Telecomunicaciones, quienes verificarán y validarán que el servicio se preste de acuerdo con lo solicitado en el anexo técnico.

3. Programa de entregas.

El Instituto requiere contar con el servicio en los sitios señalados en los Apéndices 1 y 2. El proveedor deberá cumplir en tiempo y forma con todas las actividades establecidas en los cronogramas de actividades señalados en el numeral 11, cronograma de actividades del anexo técnico.

4. Normas oficiales.

El posible proveedor deberá presentar las certificaciones correspondientes para las siguientes normas:

A. ISO 9001:2008 o superior
B. ISO/IEC 27001:2005
C. ISO/IEC 20000-1:2011

Con el fin de cumplir con normas y estándares de cableado estructurado, y de esta forma asegurar que las instalaciones proporcionen la máxima vida útil y un desempeño óptimo, cada servicio de datos, debe cumplir con las normas siguientes, según corresponda:

- NOM-001. SEDE-2005. Instalaciones Eléctricas (Norma Oficial Mexicana).
- NMX-J-511-ANCE.1999 Sistema de soportes metálicos tipo charola para cables: Especificaciones y métodos de prueba.
- NMX-I-248-1998 NYCE.-2005. Cableado de Telecomunicaciones para Edificios Comerciales Especificaciones y Métodos de Prueba.
- NMX-I-279-NYCE-2001: "Telecomunicaciones-Cableado-Cableado Estructurado-b Canalización y Espacios para Cableados de Telecomunicaciones en Edificios Comerciales".
- NMX-J-023/1-1997-ANCE Productos eléctricos – Cajas registro metálicas de salida, Parte 1: Especificaciones y métodos de prueba.
- NMX-B-209-1990 y NMX-B-210-1990 Canalización (tubería).
- ANSI/EIA/TIA-568B.1, B.2 y B.3 y adenda: B.1-1, B.2-2, B.2-3, B.2-4, B.3-1 Norma para Cableado de Telecomunicaciones en edificios comerciales.
- ANSI/EIA/TIA-569A Norma para espacios y canalizaciones de cableado de Telecomunicaciones en edificios comerciales. Febrero de 1997.
- ANSI/EIA/TIA-606. Norma para la Administración de Infraestructura de Telecomunicaciones en edificios comerciales. Febrero 1993.
- ANSI/EIA/TIA-606-A. Norma para la Administración de Infraestructura de Telecomunicaciones en edificios comerciales. Mayo 2002.
- J-STD-607-A. Requerimientos de tierra y conexión a tierra en edificios comerciales para Telecomunicaciones. Octubre 2002.
- ISO/IEC FDIS 11801: 2002 (E) Cableados Estructurados Genéricos.

Las áreas que brindarán el servicio de SOC al IMSS deberán estar certificadas en ISO/IEC 27001:2005.

5. Licencia, Permisos, Folletos, Catálogos.

1) El proveedor de la partida 1 deberá contar con:

A. Copia simple del título de concesión vigente por parte de la SCT o autoridad competente para enlaces de comunicaciones.
B. Certificado de homologación de los componentes de la Estación Terrena-Telepuerto.
C. Certificado de homologación de los componentes de la Estación Terrena Remota-VSAT.
D. Certificación del fabricante en el equipo que conforma la propuesta técnica, en la cual detalle lo siguiente: Distribuidor autorizado con capacidad de instalar y operar la infraestructura propuesta.

2) El proveedor de la partida 2 deberá contar con:

A. Una o varias concesiones de red pública de telecomunicaciones o concesiones que le permitan prestar los servicios de telecomunicaciones objeto de esta partida 2 de la contratación otorgada(s) por la Secretaría de Comunicaciones y Transportes y/o el Instituto Federal de Telecomunicaciones, debiendo dichas concesiones tener autorizada la prestación de los servicios y tener una cobertura nacional.
B. Infraestructura propia para poder ofrecer acceso a la red de Internet de manera directa, con la posibilidad de ofertar incrementos y decrementos de ancho de banda por consumo y con la garantía de Niveles de Servicio que satisfagan los requerimientos del IMSS, y
C. Con una constancia de registro de servicios de valor agregado para el acceso a internet.
D. Los servicios de esta partida 2 serán rematados en las ubicaciones definidas en los Apéndices de este anexo técnico, considerando que al menos parte de estos servicios serán solicitados en el centro de datos en el que se aloja la infraestructura "Nube IMSS Digital", provista por el Instituto para los fines ya comentados.

6. Visitas a instalaciones.

No aplica.

7. Plazo para la prestación del servicio.

El IMSS requiere los servicios objeto del presente procedimiento a partir del día siguiente de la notificación de la adjudicación y hasta el 31 de diciembre de 2020.

8. Lugar de entrega.

El proveedor se obliga proporcionar el servicio en los sitios señalados los Apéndices 1 y 2, deberá activar los servicios conforme a lo señalado en el anexo técnico.

9. Condiciones de la prestación del servicio.

PARTIDA 1

El Instituto requiere una red privada que proporcione el servicio a los sitios señalados en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual.", el cual ya sea de manera terrestre o satelital, deberá otorgar lo siguiente:

(i) Proporcionar los servicios de red de transporte de datos para el tráfico de datos que genere el Instituto, así como ofrecer la infraestructura necesaria e instalación de la misma para proporcionar dicho servicio.
(ii) Proporcionar el mantenimiento y soporte a la infraestructura de comunicaciones del servicio que corresponda a los componentes que el proveedor utilice para la entrega del mismo, el cual será de acuerdo a su estrategia de mantenimiento y soporte para garantizar los niveles de servicio solicitados.
(iii) Proporcionar un centro de monitoreo para los servicios señalados en el punto (i) que contemple los siguientes servicios y/o actividades:
    - Cumplimiento de Niveles de Servicio.
    - Mesa de Servicios.
    - Información Ejecutiva.
    - Repositorio de Información.

PARTIDA 2
El proveedor deberá proporcionar el servicio de acceso a la red de Internet, para los nodos o inmuebles identificados en el Apéndice 2, sección en donde se define la capacidad requerida para cada uno de los nodos en cuestión. El servicio de acceso a Internet deberá proporcionarse conforme a los niveles de servicio establecidos en el presente documento.

El alcance de los servicios suministrados por el proveedor incluirá funcionalidades y servicios administrados de seguridad en cada uno de los 3 nodos listados en el Apéndice 2 "Inventario de Servicios de Acceso a Internet", mismos que con excepción del atributo de "Clean Pipes" (Capacidad de Mitigación de Ataques de Negación de Servicio) que debe estar integrado a cualquier Servicio de Acceso a Internet en los 3 nodos, serán cotizados de manera desagregada al servicio administrado de acceso a Internet (medio y acceso), tal y como se observa en el Anexo Técnico.

Se deberá complementar la mitigación en la nube con la protección anti-DDoS en sitio para los portales web descritos en el anexo, incluyendo todos los elementos para la protección Web de los portales descritos en el anexo.

10. Documento que se levantará para hacer constar la prestación del servicio.

PARTIDA 1
Para hacer constar que la prestación del servicio se llevó a cabo a entera satisfacción del Instituto, el proveedor deberá elaborar la siguiente documentación:

- Sitios terrestres: Protocolo de Pruebas para la Entrega de Sitios Terrestres Tipo A, (Anexo 2).
- Sitios satelitales: Protocolo de Pruebas para la Entrega de Sitios Satelitales Tipo B, (Anexo 3).

Ambos documentos se adjuntan al presente anexo y deberán ser entregados al Administrador del Contrato debidamente requisitados y firmados por el proveedor y por el Instituto.

Asimismo, el proveedor deberá entregar al Instituto un reporte de avance semanal del servicio y demás documentación que señala el anexo técnico, dichos reportes deberán ser por escrito, con acuse de recibo y deberán contener el avance pormenorizado de la preparación y ejecución de cada una de las etapas para suministrar el servicio.

El Instituto considerará que el servicio efectivamente prestado está disponible cuando opere correctamente bajo los requerimientos solicitados en el anexo técnico.

PARTIDA 2

Para hacer constar que la prestación del servicio se llevó a cabo a entera satisfacción del Instituto, el proveedor deberá elaborar la documentación referida en el anexo técnico:

- Entregables por Única Vez
- Entregables Periódicos
- Reportes en Línea

11. Tipo de abastecimiento.

Una sola fuente de prestación de servicio.

12. Garantías.

El proveedor para garantizar el cumplimiento de todas y cada una de las obligaciones estipuladas en el contrato, deberá presentar en la División de Contratos dependiente de la Coordinación Técnica de Planeación y Contratos, de la Coordinación de Adquisición de Bienes y Contratación de Servicios de la entidad contratante, póliza de fianza en la misma moneda en que se cotizó el servicio, expedida por afianzadora debidamente constituida en términos de la Ley Federal de Instituciones de Fianzas, dentro de los 10 (diez) días naturales siguientes a la firma del contrato respectivo, para garantizar el cumplimiento de todas y cada una de las obligaciones a su cargo derivadas del contrato, a favor del IMSS, por un monto equivalente al 10% sobre el importe total adjudicado, sin incluir el I.V.A. y/o IEPS, según sea el caso, en moneda nacional, de conformidad con lo establecido en el artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como en el numeral 75 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro social vigente.

En apego al artículo 87 del Reglamento de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público, por tratarse de una contratación que abarca más de un ejercicio fiscal, la garantía de cumplimiento del contrato podrá ser por el porcentaje que corresponda del monto total por erogar en el ejercicio fiscal de que se trate, y deberá ser renovada cada ejercicio fiscal por el monto que se ejercerá en el mismo, la cual deberá presentarse a la dependencia o entidad contratante a más tardar dentro de los primeros diez días naturales del ejercicio fiscal que corresponda. La renovación señalada deberá realizarse conforme a lo dispuesto por la fracción II y el último párrafo del artículo 103 del presente Reglamento.

La garantía de cumplimiento a las obligaciones del contrato, únicamente podrá ser liberada mediante autorización que sea emitida por escrito, por parte del Instituto en forma inmediata, siempre y cuando el proveedor haya cumplido a satisfacción del Instituto con todas las obligaciones contractuales, para lo cual deberá presentar mediante escrito la solicitud de liberación de la fianza en la División de Contratos.

Se hará efectiva la garantía relativa al cumplimiento del contrato:

- Cuando el proveedor incumpla con cualquiera de las obligaciones establecidas en el contrato que se celebre.
- Cuando se rescinda administrativamente el contrato.
- La ejecución de las garantías será con independencia de la aplicación de las penas convencionales y deducciones que procedan y de la rescisión administrativa del contrato.

Además de las sanciones anteriormente mencionadas, serán aplicables las que estipulen las disposiciones legales vigentes en la materia.

La ejecución de la garantía de cumplimiento del contrato será proporcional al monto de las obligaciones incumplidas.

13. Forma de pago.

El servicio descrito en el anexo técnico está modelado con base en un esquema de pago unitario mensual, modalidad que permitirá el cálculo mensual de la factura del proveedor por cada uno de los conceptos del servicio que haya entregado durante el mes y estén funcionando de acuerdo al catálogo descrito con detalle en el anexo técnico. Para fines de facturación, el Instituto considerará a los meses con 30 días, salvo aquellos casos en los que existan entregas parciales, es decir, sólo se considerarán para fines de facturación los días de servicio efectivamente prestados.

Bajo este esquema, el proveedor debe reportar y solicitar al Instituto el pago asociado al servicio que éste ha entregado y que esté funcionando conforme a las especificaciones descritas en el anexo técnico, y con estricto apego a las características y niveles de servicio que se requieren para cada rubro definido, sujeto a posibles deducciones por incumplimiento de los mismos, por lo que el IMSS, a través del Administrador del Contrato, evaluará las condiciones de funcionalidad y operatividad de los servicios entregados por el proveedor para que proceda el pago mensual que debe efectuarse por los mismos.

El detalle de las condiciones y procedimiento que habrá de seguirse para efectuar el pago de los servicios objeto de este contrato se encuentra descrito a continuación:

El Instituto realizará por concepto del servicio, pagos mensuales dentro de los 20 (veinte) días posteriores a la presentación, validación y aceptación de los servicios por parte del Administrador del Contrato, así 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 proveedor deberá contar previamente con los anexos 2 y 3, así como el acta de aceptación mensual elaborada y firmada por el proveedor por la entrega del servicio, avalada por el Administrador del Contrato, en la que conste la aceptación de la prestación del servicio referido a entera satisfacción del Instituto.

El proveedor deberá entregar oportunamente la factura por los servicios devengados del mes, en la Coordinación Técnica de Servicios Administrativos de la Dirección de Innovación y Desarrollo Tecnológico, ubicada en Calle de Tokio 80, 5° piso, Colonia Juárez, Delegación Cuauhtémoc, Código Postal 06600, Ciudad de México, 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.

Para el trámite de pago el proveedor deberá expedir sus comprobantes fiscales digitales en el esquema de facturación electrónica, con las especificaciones normadas por el Sistema 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 476, Colonia Juárez, C.P. 06600, Delegación Cuauhtémoc, Ciudad de México, para la validación de dichos comprobantes el proveedor deberá cargar en Internet, a través del Portal de Servicios a Proveedores de la página del Instituto el archivo en formato XML; la validez de los mismos será determinada durante la carga y únicamente los comprobantes validos serán procedentes para pago.

El proveedor se obliga a no cancelar ante el SAT los comprobantes fiscales digitales a favor del Instituto, previamente validados en el portal de servicios a proveedores, salvo comunicación y autorización expresa, por parte del el Instituto, a través del Administrador del Contrato, de la justificación y reposición en su caso.

El pago de los servicios se efectuará en pesos mexicanos, a los 20 días naturales posteriores a la entrega de la representación impresa del comprobante fiscal digital y documentación comprobatoria que acredite la entrega de los servicios de conformidad con lo normado en el "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y constitución de fondos fijos", en la División de Trámite de Erogaciones de la Coordinación de Contabilidad y Trámite de Erogaciones, dependiente de la Dirección de Finanzas, sita Calle Gobernador Tiburcio Montiel No. 15, Col. San Miguel Chapultepec, Delegación Miguel Hidalgo, Ciudad de México, C. P. 11850, de lunes a viernes en un horario de 9:00 a 14:00 horas, previa validación y autorización que para tal efecto realice el Titular de la División de Telecomunicaciones en su carácter del Administrador del Contrato y la Coordinación de Sistemas de Infraestructura Tecnológica Institucional.

Las facturas que amparen bienes y 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.

El proveedor deberá entregar los siguientes documentos:

- Original y copia de la factura electrónica que expida el proveedor a nombre del Instituto, con domicilio fiscal en Av. Paseo de la Reforma núm. 476, Colonia Juárez, Delegación Cuauhtémoc C.P. 06600, México, D.F., y RFC IMS-421231-I45, que reúna los requisitos fiscales, en la que se indiquen los servicios prestados, número de proveedor, número de contrato, número de fianza y denominación social de la Afianzadora; así como el reporte del servicio prestado, elaborado y firmado por el área usuaria y/o el Administrador del Contrato.
- El proveedor deberá expedir 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 fiscalmente validas serán procedentes para pago. El proveedor deberá proporcionar a las áreas financieras 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.
- En caso de que el proveedor presente su factura con errores o deficiencias, éstos se le harán saber por parte del Instituto dentro del término estipulado para ello, y el plazo de pago se ajustará en términos del artículo 90 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. el proveedor podrá consultar esta información en la liga: https://201.144.108.83:8443/Pagos_Prov/faces/index.xhtml., la cual permanecerá publicada hasta la fecha de vencimiento que tenía programado el contra recibo. Lo anterior permitirá que el proveedor a las 72 horas posteriores a la expedición de contra recibo, cuente con la información sobre la procedencia o improcedencia de su trámite.
- Original y copia del contrato suscrito con el IMSS.
- Copia de la garantía de cumplimiento del contrato (póliza de fianza).
- En caso de aplicar, el proveedor deberá de entregar nota de crédito a favor del el Instituto por el importe de la aplicación de la pena convencional por atraso o deductivas por la deficiencia del servicio.
- El proveedor deberá entregar al Instituto la "Opinión de Cumplimiento de Obligaciones en materia de Seguridad Social" vigente y positiva. La "Opinión de Cumplimiento de Obligaciones en materia de Seguridad Social" tendrá una vigencia de 30 días naturales a partir del día de su emisión. En caso

que el proveedor no adjunte la "Opinión de Cumplimiento de Obligaciones en materia de Seguridad Social" o no esté vigente y/o sea negativa, no se recibirá su documentación, e informará que deberá obtener la citada Opinión, o en caso que sea negativa, que puede presentar aclaración o pagar sus créditos fiscales ante la Subdelegación que le corresponda o en caso que no esté vigente, que deberá obtenerla nuevamente.

El pago se realizará mediante transferencia electrónica de fondos, a través del esquema electrónico interbancario que el Instituto tiene en operación, para tal efecto el proveedor se obliga a proporcionar en su oportunidad el número de cuenta, CLABE, Banco y Sucursal a nombre del el proveedor, a menos que el proveedor acredite en forma fehaciente la imposibilidad para ello.

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

Asimismo, el Instituto podrá aceptar a solicitud del proveedor que en el supuesto que tenga cuentas liquidas y exigibles a su cargo, aplicarlas contra los adeudos que, en su caso, tuviera por concepto de cuotas obrero-patronales, conforme a lo previsto en el artículo 40 B de la Ley del Seguro Social, adicionalmente el proveedor acepta se realicen las deducciones correspondientes en su caso, generados por la aplicación de penas convencionales derivados de atrasos o deductivas por la deficiencias en el servicio.

El proveedor que celebre contrato de cesión de derechos de cobro, deberá notificarlo por escrito al Instituto, con un mínimo de cinco días naturales anteriores a la fecha de pago programada, entregando invariablemente los documentos sustantivos de dicha cesión, asimismo el proveedor podrá optar por cobrar a través de factoraje financiero conforme al Programa de Cadenas Productivas de Nacional Financiera, S.N.C. Institución de Banca de Desarrollo con el Instituto.

En caso que el proveedor reciba pagos en exceso deberá reintegrar dichas cantidades más los intereses correspondientes, conforme a la tasa que establezca la Ley de Ingresos de la Federación, para los casos de prórroga cuando existan 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 ponga efectivamente las cantidades a disposición del el Instituto.

El proveedor deberá facturar mensualmente, por periodos mensuales vencidos de servicio, en los primeros diez días naturales del mes siguiente, debiendo entregar al Instituto: la(s) factura(s) correspondiente(s) al servicio, de acuerdo con lo siguiente:

A. El proveedor entregará la factura a la Coordinación Técnica de Servicios Administrativos de la DIDT.
B. La Coordinación Técnica de Servicios Administrativos envía factura a la Coordinación de Sistemas de Infraestructura Tecnológica Institucional.
C. La Coordinación de Sistemas de Infraestructura Tecnológica Institucional envía a la División de Telecomunicaciones la factura para su validación e integración del sustento documental.
D. El Administrador del Contrato integra los respectivos sustentos documentales incluyendo las deducciones y penas convencionales conducentes.
E. La Coordinación de Sistemas de Infraestructura Tecnológica Institucional y/o la División de Telecomunicaciones, enviarán la documentación completa a la Coordinación Técnica de Servicios Administrativos para la gestión de pago.
F. La Coordinación Técnica de Servicios Administrativos entregará factura al proveedor.

G. El proveedor deberá ingresar su factura y documentación correspondiente al área de Trámite de Erogaciones para los trámites correspondientes.

El pago de los servicios quedará condicionado proporcionalmente al pago que el proveedor deba efectuar por concepto de penas convencionales por atraso.

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

14. Vigencia del contrato.

El IMSS requiere los servicios objeto del presente procedimiento a partir del día siguiente de la notificación de la adjudicación y hasta el 31 de diciembre de 2020.

15. Mecanismos de supervisión y verificación de los servicios contratados.

PARTIDA 1

El Instituto solo recibirá o aceptará el servicio, previa verificación y cumplimiento de las especificaciones requeridas, de conformidad con la siguiente documentación:

- Sitios terrestres: Protocolo de Pruebas para la Entrega de Sitios Terrestres Tipo A, (Anexo 2).
- Sitios satelitales: Protocolo de Pruebas para la Entrega de Sitios Satelitales Tipo B, (Anexo 3).

Ambos documentos deberán ser entregados al Administrador del Contrato debidamente requisitados y firmados por el proveedor y por el Instituto.

Asimismo, el proveedor deberá entregar al Instituto un reporte de avance semanal del servicio y demás documentación que señala el anexo técnico, dichos reportes deberán ser por escrito, con acuse de recibo y deberán contener el avance pormenorizado de la preparación y ejecución de cada una de las etapas para suministrar el servicio.

En tal virtud, el proveedor acepta expresamente que hasta en tanto no se cumpla de conformidad con lo establecido en los párrafos anteriores, el servicio no se tendrá como aceptado o recibido por parte del Instituto.

PARTIDA 2

Para hacer constar que la prestación del servicio se llevó a cabo a entera satisfacción del Instituto, el proveedor deberá elaborar la documentación referida en el anexo técnico:

- Entregables por Única Vez
- Entregables Periódicos
- Reportes en Línea

16. Criterio de evaluación.

PARTIDA 1. SERVICIO ADMINISTRADO DE RED PRIVADA VIRTUAL

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

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

PARTIDA 2.- SERVICIO ADMINISTRADO DE ACCESO A INTERNET.

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

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

17. Tipo de contrato.

Para ambas partidas, el contrato a celebrarse entre el Instituto y el proveedor será abierto, esto es, bajo demanda, y tendrá una duración a partir del día siguiente de la notificación de la adjudicación y hasta el 31 de diciembre de 2020. Los precios serán fijos y permanecerán durante la vigencia del contrato.

18. Penas convencionales.

De conformidad con lo establecido en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como en los numerales 5.5.7. y 5.5.7.1. de las Políticas, Bases y Lineamientos en Materia de Adquisiciones y de Prestación de Servicios del IMSS, la penalización se calculará a partir del día siguiente en que concluye el plazo o fecha convenida para iniciar la prestación del servicio, de acuerdo a los términos y condiciones expresados en la siguiente fórmula:

Pca=%d x nda x vspa

Dónde:

%d = porcentaje determinado en la convocatoria.

Pca = pena convencional aplicable.

nda = número de días de atraso.

vspa = valor de los servicios prestados con atraso, sin IVA.

PARTIDA 1

En la tabla 1, se describen las penas convencionales correspondientes al servicio.

No.	Concepto	Nivel del servicio	Pena
1	Inicio mesas de trabajo	Atraso en el cumplimiento de la entrega del servicio	2.5% (dos punto cinco por ciento) por cada día natural de atraso sobre el valor total máximo del contrato.
2	Por suspensión o atraso en la entrega del servicio	Atraso en el cumplimiento de la entrega del servicio. .	2.5% (dos punto cinco por ciento) sobre el valor de los servicios entregados en forma extemporánea, multiplicado por el número de días naturales transcurridos desde el vencimiento hasta la entrega.
3	Centro de Monitoreo	Incumplimiento en el plazo de entrega del centro de monitoreo señalado en el anexo técnico.	2.5% del monto mensual del servicio no entregado.

Tabla 1

En cualquier caso, dicha pena no podrá exceder del monto de la garantía de cumplimiento del contrato o pedido, o del 20% del monto de los bienes o servicios no prestados fuera del plazo convenido, cuando se hubiere exceptuado de la presentación de la garantía.

PARTIDA 2

Penas convencionales por incumplimiento de las fechas pactadas para la ejecución de los servicios:
Por suspensión o atraso en la entrega del servicio, el Instituto sancionará con una pena convencional equivalente al 2.5% (dos punto cinco por ciento) sobre el valor de los servicios entregados en forma extemporánea, multiplicado por el número de días naturales transcurridos desde el vencimiento hasta la entrega.

La pena convencional por atraso se calculará por cada día de incumplimiento, de acuerdo con el porcentaje de penalización establecido en el párrafo anterior, aplicado al valor del servicio prestado con atraso y de manera proporcional al importe de la garantía de cumplimiento.

Penas contractuales por no presentarse a la reunión para el inicio de las mesas de trabajo.
En caso que el proveedor adjudicado no se presente en la fecha pactada en el documento denominado anexo técnico, se sancionará con una pena contractual equivalente al 2.5% (dos punto cinco por ciento) por cada día natural de atraso sobre el valor total máximo del contrato.

El proveedor adjudicado autoriza a descontar las cantidades que resulten de aplicar las sanciones señaladas en párrafos anteriores, sobre los pagos que a él deberán de cubrirse, durante el período en que incurra y/o se mantenga el incumplimiento con motivo de la prestación del servicio.

La suma de las penas convencionales no deberá exceder el importe de la garantía de cumplimiento.

19. Deductivas.
Se aplicará lo indicado en las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto establecidos en el punto 5.5.7.2. Deducciones al Pago de cualquier tipo de servicios, el cual indica: En el procedimiento para la aplicación de las deducciones para los contratos de prestación de servicios, el Administrador del Contrato será responsable de calcular y aplicar la deducción por prestación deficiente del servicio.

Los niveles de disponibilidad se refieren a la cantidad mensual del servicio efectivamente proporcionado al Instituto por parte del proveedor. Estos niveles se expresan en porcentaje como la relación del tiempo (en minutos) del servicio efectivamente proporcionado entre el total de minutos que tiene en promedio un mes. De esta forma los niveles de disponibilidad indican el porcentaje mensual del servicio mínimo requerido que el proveedor tiene que cumplir para no incurrir en deductivas.

PARTIDA 1

Para vigilar el cumplimento de los niveles de disponibilidad, el Instituto establece el Porcentaje de Disponibilidad Medio mensual (PDn), cuya variable permite medir la cantidad del servicio efectivamente proporcionado al Instituto y que servirá de base para el cálculo de las deductivas aplicables. El cálculo del Porcentaje de Disponibilidad Medio mensual se calculará con la siguiente formula:

PDn = [1 – (TNDn / TDn)] x 100

ANEXOS
DIVISIÓN DE CONTRATOS

Dónde:
PDn: Es el porcentaje de disponibilidad medio mensual
TNDn: Es el tiempo en minutos, durante horas naturales del mes, que el servicio no estuvo disponible (tiempo de falla del servicio)
TDn: Es el tiempo en minutos del total de horas naturales del mes

En caso que el porcentaje de disponibilidad media mensual PDn sea menor que los niveles de disponibilidad del servicio, el proveedor incurrirá en deductivas. Para tal efecto se establece la Unidad Porcentual de Deductivas (UDn) del **0.56%.**

En la tabla 2, se describen las deductivas que se aplicarán de manera independiente para cada uno de los niveles de disponibilidad.

No.	Concepto	Nivel del servicio	Deductiva
1	Enlaces terrestres	Disponibilidad de enlaces terrestres, 98.89%	Deductiva=((Dm – PDn) / UDn)*(PCn*Costo) Dónde: Dm: Disponibilidad mínima (siempre será 98.89%) PDn: Porcentaje de Disponibilidad medio mensual UDn: Unidad Porcentual de Deductivas **(0.56%)** PCn: Pena convencional (2.0% del costo mensual del servicio en cuestión) Costo: Costo mensual del servicio
2	Enlaces satelitales	Disponibilidad de enlaces satelitales, 98.89%	Deductiva=((Dm – PDn) / UDn)*(PCn*Costo) Dónde: Dm: Disponibilidad mínima (siempre será 98.89%) PDn: Porcentaje de Disponibilidad medio mensual UDn: Unidad Porcentual de Deductivas **(0.56%)** PCn: Pena convencional (2.0% del costo mensual del servicio en cuestión) Costo: Costo mensual del servicio
3	Mesa de servicios	Disponibilidad de mesa de servicios, 7x24x365	Deductiva=((Dm – PDn) / UDn)*(PCn*Costo) Dónde: Dm: Disponibilidad mínima (siempre será 98.89%) PDn: Porcentaje de Disponibilidad medio mensual UDn: Unidad Porcentual de Deductivas **(0.56%)** PCn: Pena convencional (2.0% del costo mensual del servicio en cuestión) Costo: Costo mensual del servicio

Tabla 2

En cualquier caso, dicha deducción no podrá exceder del monto de la garantía de cumplimiento del contrato o pedido o del 20% del monto total de los bienes o servicios contratados, cuando se hubiere exceptuado de la presentación de la garantía.

PARTIDA 2

En la tabla 3, se describen las deductivas que se aplicarán de manera independiente para cada uno de los niveles de disponibilidad sobre los Servicios Administrados de Acceso a Internet.

Tipo de Nivel de Servicio	Descripción de Nivel de Servicio	Métrica Objetivo Mensual	Deductiva Mensual Aplicable	Cómputo de la Deductiva
Disponibilidad	Disponibilidad de los Servicios Administrados de Acceso a Internet (por Nodo)	99.98%	0.01 (1 por ciento) por cada minuto de indisponibilidad en el mes, fuera de la métrica objetivo	Por cada minuto de indisponibilidad en el nodo por debajo de la métrica, se deducirá 1% de la facturación mensual de dicho servicio (nodo)
Disponibilidad	Disponibilidad del Servicio de Prevención de Intrusos (IPS)	99.96%	0.001 (1 al millar) por cada minuto de indisponibilidad en el mes, fuera de la métrica objetivo	Por cada minuto de indisponibilidad en cada nodo por debajo de la métrica, se deducirá 0.1% de la facturación mensual del Servicio Administrado de Acceso a Internet para el nodo específico
Disponibilidad	Disponibilidad del Servicio de Firewall en Alta Disponibilidad	99.96%	0.001 (1 al millar) por cada minuto de indisponibilidad en el mes, fuera de la métrica objetivo	Por cada minuto de indisponibilidad en cada nodo por debajo de la métrica, se deducirá 0.1% de la facturación mensual del Servicio Administrado de Acceso a Internet para el nodo específico
Disponibilidad	Disponibilidad del Servicio de Análisis de Flujo	99.96%	0.001 (1 al millar) por cada minuto de indisponibilidad en el mes, fuera de la métrica objetivo	Por cada minuto de indisponibilidad en cada nodo por debajo de la métrica, se deducirá 0.1% de la facturación mensual del Servicio Administrado de Acceso a Internet para el nodo específico
Disponibilidad	Disponibilidad del Servicio de Control de Acceso a Páginas Web	99.96%	0.001 (1 al millar) por cada minuto de indisponibilidad en el mes, fuera de la métrica objetivo	Por cada minuto de indisponibilidad en cada nodo por debajo de la métrica, se deducirá 0.1% de la facturación mensual del Servicio Administrado de Acceso a Internet para el nodo específico
Disponibilidad	Disponibilidad del Servicio de Análisis de Vulnerabilidades	99.96%	0.001 (1 al millar) por cada minuto de indisponibilidad en el mes, fuera de la métrica objetivo	Por cada minuto de indisponibilidad en cada nodo por debajo de la métrica, se deducirá 0.1% de la facturación mensual del Servicio Administrado de Acceso a Internet para el nodo específico
Disponibilidad	Disponibilidad del Servicio de Proxy	99.96%	0.001 (1 al millar) por cada minuto de indisponibilidad en el mes, fuera de la métrica objetivo	Por cada minuto de indisponibilidad en cada nodo por debajo de la métrica, se deducirá 0.1% de la facturación mensual del Servicio Administrado de Acceso a Internet para el nodo específico
Entrega	Entrega de modificaciones en Ancho de Banda de Internet	95% de las veces en 4 horas o menos	0.001 (1 al millar) por cada hora de retraso fuera de la métrica objetivo en el mes	Por cada hora de retraso en la entrega de modificaciones en ancho de banda de Internet, fuera de la métrica objetivo, se deducirá 0.1% de la facturación mensual del Servicio Administrado de Acceso a Internet para el nodo específico
Desempeño	Latencia	Menor a 100 milisegundos de ida y	0.002 (2 al millar) por cada milisegundo que, en promedio	Por cada milisegundo que, en el promedio mensual de la Latencia del Servicio de Acceso a Internet, se

ANEXOS
DIVISIÓN DE CONTRATOS

	vuelta al Punto de Acceso a la Red más cercano	mensual, exceda el Servicio Administrado de Acceso a Internet, en el nodo específico, respecto de la métrica exigida	exceda la métrica exigida, se deducirá 0.2% de la facturación de dicho nodo en dicho mes

Tabla 3

La deductiva máxima aplicable está acotada al costo mensual asociado del sitio y el mes correspondiente en el que el licitante ganador incurrió en el incumplimiento de los niveles de servicio.

20. Mecanismos de control para la administración del contrato

20.1 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 posible proveedor, incurra en incumplimiento de cualquiera de las obligaciones a su cargo, de conformidad con el procedimiento siguiente.

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

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 posible proveedor. La determinación de dar o no por rescindido el contrato deberá ser debidamente fundada, motivada y comunicada al proveedor 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 posible proveedor, hasta el momento en que se determine la rescisión administrativa.

En el supuesto de que se rescinda el contrato, el Instituto, no aplicará las penas convencionales, ni su contabilización, para hacer efectiva la garantía de cumplimiento de este instrumento jurídico. Iniciado un procedimiento de conciliación el Instituto, bajo su responsabilidad podrá suspender el trámite del procedimiento de rescisión.

Si previamente a la determinación de dar por rescindido el contrato, el posible proveedor, está en condiciones óptimas para continuar proporcionando el servicio, el procedimiento iniciado quedará sin efectos, previa aceptación y verificación del Instituto, por escrito, de que continúa vigente la necesidad de contar con los servicios, en su caso, las penas convencionales correspondientes.

El Instituto, podrá determinar no dar por rescindido el contrato, cuando durante el procedimiento advierta que dicha rescisión pudiera ocasionar algún daño o afectación a las funciones que tiene encomendadas. En este supuesto, el Instituto, elaborará un dictamen en el cual justifique que los impactos económicos o de operación

que se ocasionarían con la rescisión del contrato resultarían más inconvenientes.

De no darse por rescindido el contrato, el Instituto, establecerá de conformidad con el posible proveedor, un nuevo plazo para el cumplimiento de aquellas obligaciones que se hubiesen dejado de cumplir, a efecto de que el posible proveedor, subsane el incumplimiento que hubiere motivado el inicio del procedimiento de rescisión. Lo anterior, se llevará a cabo a través de un convenio modificatorio en el que se atenderá a las condiciones previstas en los dos últimos párrafos del artículo 52, de la 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 posible proveedor adjudicado incurra en cualquiera de las causales siguientes.

- Cuando no entregue la garantía de cumplimiento del contrato, dentro del término de diez días naturales posteriores a la firma del mismo.
- Cuando incurra en falta de veracidad total o parcial respecto a la información proporcionada para la adjudicación o formalización del contrato.
- Cuando incumpla, total o parcialmente, con cualesquiera de las obligaciones derivadas de la adjudicación del contrato de la presente licitación.
- Cuando se compruebe que el posible proveedor adjudicado realice el servicio con especificaciones y características distintas a las solicitadas en esta licitación.
- Cuando transmita total o parcialmente, bajo cualquier título, los derechos y obligaciones derivados del contrato, con excepción de los derechos de cobro, previa autorización del Instituto.
- Sea declarado en concurso mercantil o cualquier situación análoga o equivalente que afecte el patrimonio del posible proveedor.
- Cuando de manera reiterativa y constante, el posible proveedor 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.
- Si la Comisión Federal de Competencia, de acuerdo a sus facultades, notifica al Instituto la sanción impuesta al proveedor, 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.

20.2. 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 SFP. En estos casos el Instituto reembolsará al posible proveedor, 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 de la presente licitación.

21. Área técnica encargada de verificar la prestación del servicio
El Titular de la Coordinación Técnica de Redes y Telecomunicaciones y el Titular de la División de Telecomunicaciones.

22. Responsable de la evaluación de las propuestas técnicas.
Titular de la División de Telecomunicaciones.

23. Administrador del contrato y responsable de la supervisión del servicio.
El Titular de la Coordinación de Sistemas de Infraestructura tecnológica Institucional

24. Firmas del documento.

Responsable de Elaboración

ING. JOSÉ CARLOS ARAGÓN HERRERA
ENCARGADO DEL DESPACHO DE LA DIVISIÓN DE TELECOMUNICACIONES DE CONFORMIDAD CON EL OFICIO NO. 09 52 76 61 5300/202000121, DE FECHA 28 DE FEBRERO DE 2020.

Responsable de Revisión

ING. HUGO OLVERA ORTEGA
COORDINADOR TÉCNICO DE REDES Y TELECOMUNICACIONES

Responsable de Aprobación

ING. EDUARDO OROPEZA ORTIZ
TITULAR DE LA COORDINACIÓN DE SISTEMAS DE INFRAESTRUCTURA TECNOLÓGICA INSTITUCIONAL

IMSS	INSTITUTO MEXICANO DEL SEGURO SOCIAL DIRECCIÓN DE ADMINISTRACIÓN UNIDAD DE ADQUISICIONES E INFRAESTRUCTURA COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS	Contrato Número DC20S375

ANEXO 2

"PROPUESTA TÉCNICA, PROPUESTA ECONÓMICA Y ACTA DE ADJUDICACIÓN"

ANEXOS

DIVISÍON DE CONTRATOS

EL PRESENTE ANEXO CONSTA DE **39** HOJAS INCLUYENDO ESTA CARÁTULA

18

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

SIN TEXTO

Bestel

.com.mx

INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

SERVICIO DE COMUNICACIÓN PARA ENLACES DE CRITICIDAD MEDIA Y NORMAL DEL IMSS

PROPUESTA TÉCNICA

ANEXOS

DIVISIÓN DE CONTRATOS

12

Contenido

1. **Objetivo del documento**
   Operbes S.A. de C.V. tomó en consideración que en anexo técnico se estableció las especificaciones técnicas, calendarios, arquitecturas y lineamientos para la contratación del Servicio de Comunicación para Enlaces de Criticidad Media y Normal del IMSS, el cual incluye los siguientes servicios:

   - Partida 1: Servicio Administrado de Red Privada Virtual.
   - Partida 2: Servicio Administrado de Acceso a Internet.

   ANEXOS
   DIVISIÓN DE CONTRATOS

   Clave CUCOP: 31600001

2. **Objetivo**
   Contar con servicios administrados que presten al IMSS, de manera integrada y unificada, el suministro, configuración, operación, administración y soporte de Red Privada Virtual y Acceso a Internet, incluyendo el monitoreo y gestión.

   Operbes S.A. de C.V. ofertará, detallará y describirá en su propuesta tanto la solución ofertada, como los alcances del servicio descritos en el presente documento, no solo repitiendo los compromisos, sino que también se detallan las herramientas tecnológicas, recursos tecnológicos, humanos y materiales que se utilizarán para la prestación del servicio. Operbes S.A. de C.V. tomó en consideración que si no describe y detalla los componentes ofertados de la solución y que estos cumplen con los requerimientos del anexo técnico y sus apéndices, el Instituto considerará que no cumple con lo requerido en el presente documento.

   Los servicios objeto de este contrato cubren las necesidades operativas de conectividad del IMSS en sus Unidades Médico-Administrativas del ámbito nacional en los nodos que se indican en los siguientes apéndices:

   - Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual (Operbes S.A. de C.V. no participa).
   - Apéndice 2: Inventario de Nodos para el Servicio Administrado de Acceso a Internet.

3. **Vigencia del servicio**
   Operbes S.A. de C.V. tomó en consideración que para ambas partidas la vigencia del servicio del presente procedimiento será a partir del día siguiente a la notificación de adjudicación y hasta el 31 de diciembre de 2020.

4. **Alcance**
   El IMSS tiene la necesidad de contratar los servicios descritos en el anexo técnico para los inmuebles (nodos) definidos en los apéndices 1 y 2, los cuales están identificados por un número único (ID), el cual será respetado por los licitantes para efectos de diseño, documentación, propuesta técnica y eventualmente su operación.

   Se hace del conocimiento de Operbes S.A. de C.V. que la volumetría que se proporciona en el catálogo de servicio, así como en los apéndices 1 y 2 es exclusivamente para efectos de cotización y no necesariamente reflejan los requerimientos del Instituto, por lo que dichas cantidades no se deberán considerar como las cantidades a contratar.

   Operbes S.A. de C.V. cotiza precios unitarios por cada uno de los conceptos establecidos en el formato de propuesta económica. El contrato que resulte de este proceso de contratación será abierto y los servicios serán solicitados bajo demanda, la cantidad de servicios a contratar se determinará por el presupuesto mínimo y máximo establecido, el uso de los servicios se determinará de acuerdo con las necesidades del Instituto.

5. Catálogo de Servicios

El catálogo de servicios del anexo técnico resume todos los elementos de servicio que son considerados elementos de pago en el contrato correspondiente, y todos ellos guardan relación con servicios descritos en una o varias secciones de este anexo técnico. Los costos de los servicios solicitados en este anexo técnico serán pagados por el IMSS a mes vencido. (Operbes S.A. de C.V. solo participa en partida 2).

PARTIDA	CONCEPTO	ANCHO DE BANDA	MINIMO	MAXIMO
PARTIDA 1	Enlace Satélite	1 Mbps	104	260
	Enlace Terrestre	6 Mbps	640	1600
	Enlace Terrestre	20 Mbps	24	60
	Enlace Terrestre	200 Mbps	24	60
	CENTRO DE MONITOREO	Cumplimiento de Niveles de Servicio	1	1
		Mesa de Servicios	1	1
		Información Ejecutiva	1	1
		Repositorio de Información	1	1

PARTIDA	CONCEPTO	ANCHO DE BANDA	MINIMO	MAXIMO
PARTIDA 2	Servicios Administrados de Acceso a Internet para Nodo "Nube IMSS Digital"		1	1
	Servicios Administrados de Acceso a Internet para Nodo "CeNaTI DF"		1	1
	Servicios Administrados de Seguridad de Internet para el Nodo "CeNaTI DF"		1	1
	Servicios Administrados de Acceso a Internet para Nodo "CeNaTI Monterrey"		1	1
	Servicios Administrados de Seguridad de Internet para el Nodo "CeNaTI Monterrey"		1	1

Catálogo de Servicios

6. Requerimientos técnicos

Precios Unitarios

Los precios unitarios son los valores que cuantifican el costo de cada uno de los servicios que se incluyen en el catálogo de servicios de este anexo técnico. A cada concepto de servicio corresponde uno y solo un precio unitario. Operbes S.A. de C.V. toma en cuenta que los precios unitarios serán permanentes e inamovibles a lo largo de la vigencia del contrato.

Arquitectura de referencia

El siguiente esquema resume, de manera muy sucinta y meramente referencial, los grandes flujos de interconexión existentes actualmente en el IMSS.

Como puede observarse existen 2 nubes de conectividad en la Red Privada Virtual del IMSS que atiende aproximadamente a 3,000 nodos, entre los que se encuentra toda clase de inmuebles asociados a la operación del Instituto. Más detalles de los tipos de inmueble y su orientación de negocio pueden revisarse en el Apéndice 1 de este documento.

El diagrama 1 establece de manera muy general, la arquitectura en la que actualmente el IMSS opera. El servicio a contratar para la Partida 1 en el presente procedimiento se encuentra acotado con líneas punteadas. Es importante mencionar que los inmuebles contemplados en esta contratación no son necesariamente la totalidad de inmuebles en los que el IMSS opera.

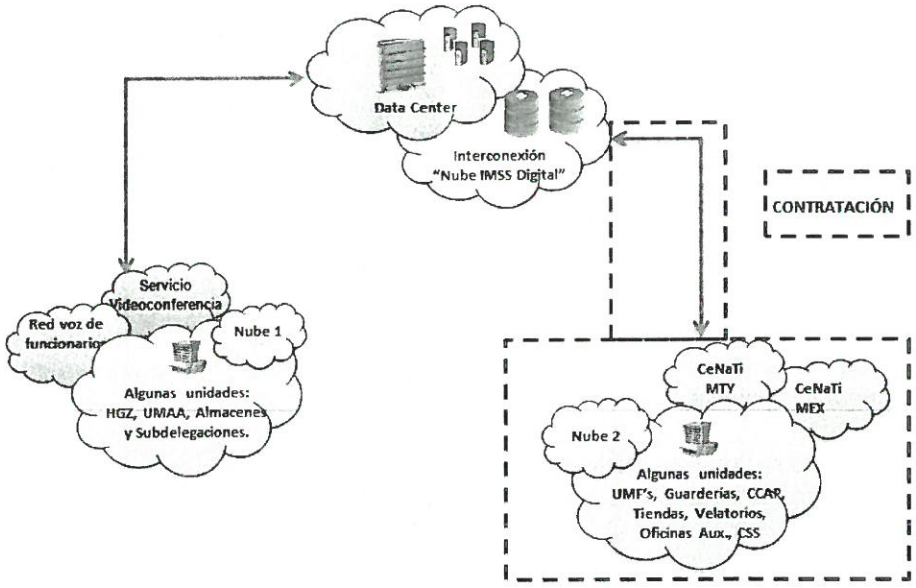


Diagrama 1

El diagrama 2 establece de manera muy general, la arquitectura en la que actualmente el IMSS opera. El servicio que se contrata para la Partida 2 en el presente procedimiento se encuentra acotado con líneas punteadas.

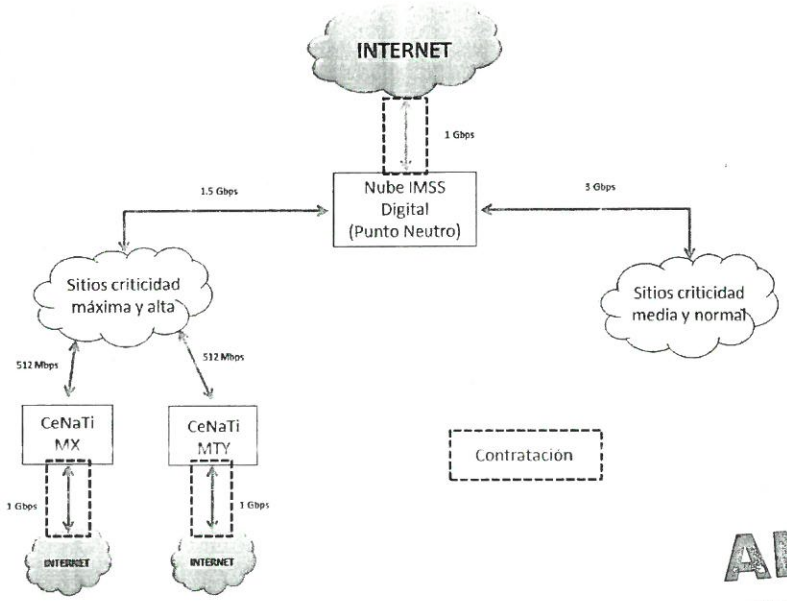


Diagrama 2

7. Especificaciones técnicas

Operbes S.A. de C.V. no participa en la Partida, por lo que no se consideran las especificaciones técnicas mencionadas a continuación:

PARTIDA 1

El servicio objeto del presente contrato se prestará como continuidad al contrato DC17S0083 y su Convenio Modificatorio No.1, por un periodo de siete meses contados a partir del día siguiente a la notificación de adjudicación y hasta el 31 de diciembre de 2020, con el proveedor que actualmente presta los servicios en el contrato DC17S0083 y su Convenio Modificatorio No.1.

7.1 Servicio Administrado de Red Privada Virtual

El Instituto requiere una red privada que proporcione el servicio a los sitios señalados en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual", la cual ya sea de manera terrestre o satelital, proporcionará lo siguiente:

(i) El servicio de red de transporte de datos para el tráfico de datos que genere el Instituto, así como ofrecer la infraestructura necesaria e instalación de esta para proporcionar dicho servicio.

(ii) El mantenimiento y soporte a la infraestructura de comunicaciones del servicio que corresponda a los componentes que Operbes S.A. de C.V. utiliza para la entrega del mismo, el cual será de acuerdo a su estrategia de mantenimiento correctivo y soporte para garantizar los niveles de servicio solicitados.

(iii) Un centro de monitoreo para los servicios señalados en el punto (i) que incluya los siguientes servicios y/o actividades:
- Cumplimiento de Niveles de Servicio.
- Mesa de Servicios.
- Información Ejecutiva.
- Repositorio de Información.

La descripción técnica del servicio se encuentra desarrollada de la siguiente forma en este anexo técnico:

A. Conformación, descripción, equipamiento y necesidades de los sitios.
B. Consideraciones del listado de sitios.
C. Descripción técnica de los enlaces para el servicio.
   i. Requisitos técnicos de los enlaces satelitales.
   ii. Requisitos técnicos de los enlaces terrestres.
D. Centro de Monitoreo.
   i. Cumplimiento de Niveles de Servicio
   ii. Mesa de Servicios
   iii. Información Ejecutiva
   iv. Repositorio de Información

A. CONFORMACIÓN, DESCRIPCIÓN, EQUIPAMIENTO Y NECESIDADES DE LOS SITIOS

El proveedor prestará el servicio para los sitios señalados en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual", por lo cual El proveedor de forma enunciativa más no limitativa proporcionará, configurará y realizará todas las actividades inherentes a la prestación del servicio.

Es importante señalar, que durante la vigencia del contrato el Instituto podrá agregar o disminuir la cantidad de sitios terrestres y satelitales.

B. CONSIDERACIONES DEL LISTADO DE SITIOS

Dentro de la propuesta técnica, El proveedor expresa de manera clara y precisa el tipo de enlace que oferta para cada sitio relacionado en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual". Para este fin, El proveedor requisitará la información solicitada para cada sitio relacionado en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual".

A continuación, se ejemplifica la información que se proporciona en el citado anexo:

Id.	SITIO	OFERTA SERVICIO MPLS (SI/NO)	TIPO ENLACE	ENTREGA MPLS EN F.O. O COBRE	COMENTARIOS (TEXTO LIBRE)
1-xxxx					

Dónde:
Id. = Identificador del sitio proporcionado por el Instituto en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual".
Sitio = Es el nombre del sitio identificado en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual"
Oferta servicio MPLS = (SI/NO) Información que proporcionará el proveedor
Tipo de enlace = Satelital o terrestre
Entrega MPLS en F.O. o cobre = Información que proporcionará el proveedor
Comentarios (texto libre) = Información que proporcionará el proveedor.

ANEXOS
DIVISIÓN DE CONTRATOS

C. DESCRIPCIÓN TÉCNICA DE LOS ENLACES PARA EL SERVICIO

Requisitos técnicos de los enlaces satelitales.

Para los enlaces satelitales, el servicio incluye, todos los elementos, recursos humanos, materiales y físicos para las actividades de continuidad del servicio, así como proporcionar todos los elementos necesarios para el servicio.

Para lograr tiempos de respuesta óptimos y cumplir con los requerimientos de latencia mínimos solicitados en este anexo técnico, el proveedor contará con la conexión directa de su POP de MPLS con el telepuerto de la solución satelital, por lo que deberá entregar en su propuesta técnica la documentación que avale el tipo de conexión y detalle de anchos de banda.

El Instituto a través del Grupo Administrador del Contrato durante la vigencia del contrato, podrá solicitar la reubicación de hasta el 10% de los enlaces satelitales a otras ubicaciones de acuerdo con las necesidades que durante la vigencia del servicio el Instituto requiera, lo anterior sin costo adicional para el Instituto.

Requisitos generales para los enlaces satelitales:

- Disponibilidad del servicio de 98.89% mensual (ver tabla 2, Niveles de servicios)
- Contar con un telepuerto satelital dentro del territorio nacional donde se recibirán, administrarán y operarán los enlaces satelitales.
- Deberá ser un sistema satelital bi-direccional.
- Los equipos de telecomunicación serán monitoreables remotamente.
- Los equipos de telecomunicación serán configurables remotamente.
- Operbes S.A. de C.V. proporcionará los servicios de conectividad satelital bidireccional de banda ancha con velocidad de recepción y transmisión de 1Mbps / 1Mbps en canal de retorno con sobresuscripción no mayor de 30 a 1, compatible con estándares de comunicación IP, el cual cuente

con codificación avanzada, técnicas de corrección de errores y funciones de seguridad que se utilicen para permitir una transmisión confiable y segura así como mecanismos de aceleración TCP/IP incorporados que permitan mejorar la experiencia del usuario. Así como una latencia máxima de 750 ms, con pérdida de paquetes menor al 1%.

- Aceleración y optimización incorporada TCP/IP para comunicación vía satélite.
- Modulación variable para garantizar la disponibilidad de los enlaces.
- Modulación variable: QPSK, 8PSK, 16APSK, 32APSK (o superior).
- El proveedor calculará las características de las portadoras de retorno con base en el cálculo de enlace. Sin embargo, se incluirán canales dinámicamente adaptativos a la modulación y el FEC dependiendo de las condiciones de operación de las estaciones terrenas remotas.
- FEC RATE (DVB-S2): 1/4,1/3,2/5,1/2,3/5,2/3,3/4,4/5,5/6,8/9,9/10.
- Consumo de potencia menor a 20 watts (lo anterior refiriéndose al radio de unidad exterior ODU).
- Rango de frecuencia de transmisión: Banda Ku.
- Los equipos soportarán vientos iguales o superiores a 70 km/h en operación.
- Temperatura de operación de ODU de -40 a 50 grados centígrados.
- Adaptabilidad portadora de retorno; soportar los modelos: AUPC, canales dinámicos y modulación/FEC. Se podrá modificar las características de la portadora de retorno, únicamente cuando la señal sea con características iguales o superiores a las antes solicitadas.
- Soportan algoritmos o herramientas que permitan incrementar la eficiencia propia de los códigos de corrección de error y mejorar la relación señal a ruido, así como ajustar dinámicamente los códigos de error y modulación de las portadoras ascendentes y descendentes a fin de mantener la disponibilidad de los enlaces durante variaciones ambientales adversas como lluvia, polvo o nieve de tal manera que se obtenga el mejor desempeño global en la red.
- Portadora de entrada con capacidad de modulación QPSK, 8APSK, con capacidad de hasta 6 Mbps.
- Esquema de acceso estándar al satélite en antena maestra (Tele Puerto): DVB-S2 con soporte a modulaciones de hasta 32APSK Y ACM, la modulación deberá de ajustarse de manera dinámica de acuerdo al ACM. Mientras que el QoS deberá ajustarse de manera dinámica al tipo de tráfico y/o aplicativos.
- La marca y el modelo del equipo de telecomunicaciones son a consideración del proveedor., siempre y cuando cumpla con lo descrito en las especificaciones del servicio.

El servicio mediante enlaces satelitales incluye:

- Antenas fijas para los sitios con un diámetro de 1.2 mts hasta 1.8 mts dependiendo de las facilidades del inmueble de acuerdo al "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual" y todo el aditamento necesario para su correcto funcionamiento, el proveedor garantizará que dicha antena sea resistente al agua, al polvo y a condiciones adversas.
- El proveedor instalará las antenas satelitales fijas junto con todos los aditamentos necesarios para su funcionamiento en los techos de los inmuebles de las unidades, el proveedor realizará cableado para conectar la antena con el módem satelital, mismo que el proveedor instalará en el interior de inmueble. Los permisos de acceso a los inmuebles para realizar estas tareas serán coordinados con el Instituto.
- Radios y/o módem, así como todo el equipamiento aplicable para el correcto funcionamiento del enlace satelital.
- Todos los cables necesarios para el correcto funcionamiento del enlace satelital.
- Instalación en caso de ser necesario, de un sistema de tierra física independiente.
- El servicio permitirá el transporte de datos para los aplicativos del Instituto.
- El proveedor proporcionará la configuración inicial y puesta a punto, así como las licencias y software que se requiera para brindar el servicio mediante enlace satelital.
- El servicio contará con las últimas versiones liberadas por el fabricante, así como el release de software, firmware y otros relacionados, éstas serán actualizadas en los equipos de telecomunicaciones durante la vigencia del contrato por el proveedor. previa coordinación con personal del Instituto y sin costo adicional para el mismo.

- Mecanismos y/o seguros contra el robo de equipos y daños que éstos pudieran sufrir por vandalismo, fenómenos naturales, accidentes, inestabilidad eléctrica o cualquier otra causa, será responsabilidad del proveedor restablecer el servicio para cumplir el nivel de servicio indicados en la tabla 2 "Niveles de servicio". Cabe señalar, que por accidente se entiende cualquier eventualidad que interrumpa la continuidad del servicio.
- El proveedor realizará todas las reparaciones que sean necesarias para garantizar la impermeabilidad de las paredes y azoteas (lozas) en los lugares que realice perforaciones para la sujeción de los equipos. De igual forma el proveedor realizará todas las reparaciones que sean necesarias para restaurar a su estado original cualquier daño que cause derivado de la instalación de los equipos propuestos para la prestación del servicio. En caso de que el proveedor no realice las reparaciones a las que hace referencia en este punto, se penalizará con una cantidad de $10,000.000 (diez mil pesos 00/100) M.N. por cada sitio que no esté reparado al momento de recibir el servicio efectivamente prestado, así como al momento de que concluya el contrato.
- Ningún sitio cuenta con sistemas de acondicionamiento de la temperatura y humedad ambientales, por lo que el proveedor tomará esto en cuenta para la selección de los equipos que integrarán su propuesta, en las que establezca condicionantes de temperatura o humedad.
- El proveedor es responsable de realizar las adecuaciones y todos los insumos y accesorios necesarios que permitan instalar adecuadamente los equipos y poner en operación el servicio y garantizar su continuidad: charolas o sujeción en pared, tornillos, cables, conectores, cinturones de plástico (cinchos), etc.
- El proveedor podrá imputar fallas del servicio por cortes en el suministro de energía eléctrica.
- En caso de que una antena se mueva o se obstruya la línea de vista con letreros u ocurra un acontecimiento semejante a los descritos, el proveedor tiene la responsabilidad de repararlos cumpliendo con los niveles de servicio descritos en este anexo técnico.
- El personal del proveedor portará en todo momento una identificación dentro de los sitios del Instituto durante el desarrollo de los trabajos necesarios para prestar el servicio.

Requisitos técnicos de los enlaces terrestres.

El servicio a través de enlace terrestre consiste en la interconexión vía MPLS (RFC 2547 de la IEFT) a través de enlaces digitales, lo cual permitirá intercambiar información a través de aplicativos propios del Instituto (voz, datos, video y colaboración).

Para los enlaces terrestres, el servicio incluye todos los elementos, recursos humanos, materiales y físicos para coordinar las actividades de continuidad del servicio, así como proporcionar todos los elementos necesarios para proporcionar el servicio, así como todo el equipo necesario, con el fin de proporcionar los servicios de conectividad con el ancho de banda solicitado en los sitios.

El proveedor cuenta con una red privada o backbone nacional propia.

El proveedor tiene **cobertura terrestre al menos del 85% de los sitios listados en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual"** con el fin de minimizar los tiempos de atención e integración de los servicios. Para los sitios terrestres no se aceptarán soluciones satelitales, inalámbricas o microondas, por lo que la solución propuesta por el proveedor. es únicamente por medio de fibra óptica o cobre.

Para el caso de nuevos requerimientos, el servicio incluye un equipo terminal (router), el cual deberá contar con al menos 1 slot disponible para ampliar la capacidad de puertos de interconexión en caso de requerirse. Este equipo debe ser nuevo y todos deberán ser de la misma marca, no se aceptan soluciones con más de una marca y deberá ser administrado y monitoreado de manera remota a través del centro de monitoreo que más adelante se especifica en este anexo técnico. La marca y el modelo del equipo de telecomunicaciones son a consideración del proveedor, siempre y cuando cumpla con lo descrito en las especificaciones del servicio.

ANEXOS

DIVISIÓN DE CONTRATOS

El servicio mediante enlaces terrestres incluye:

- La red privada del proveedor opera las 24 horas del día, los 7 días de la semana, los 365 días del año, de manera que cumpla con una disponibilidad en su backbone de al menos 98.89% mensual (ver tabla 2, Niveles de servicio).
- La red privada del proveedor soporta una conectividad conocida como any-to-any, asimismo soporta el direccionamiento IP que se designe y permitir la designación de subredes para conformar la segmentación física o lógica según sea el caso y soporta la configuración de NAT (Network Address Translation) y/o PAT (Port Address Translation). También cuenta con tiempos de latencia entre dos nodos de su backbone con valores inferiores a los 50 milisegundos considerando una trayectoria de ida y vuelta (round-trip), mientras que los valores del Jitter se encontrar por debajo de los 50 milisegundos en una dirección y pérdida de paquetes menores al 1%.
- El servicio opera con una red privada sectorial, por lo que la comunicación a cada uno de los sitios que conformen la red será de forma directa, es decir; no pasará por ningún sitio central de cualquier otra red.
- El servicio contará con las últimas versiones liberadas por el fabricante, así como el release de software, firmware y otros relacionados, éstas serán actualizadas en los equipos de telecomunicaciones durante la vigencia del contrato por el proveedor previa coordinación con personal del Instituto y sin costo adicional para el mismo.
- El Instituto podrá solicitar durante la vigencia del contrato, la reubicación de hasta el 10% de los enlaces terrestres a otras ubicaciones, lo anterior sin costo adicional para el Instituto.
- el proveedor. tomará en cuenta que el Instituto podrá solicitar enlaces terrestres de hasta 20 Mbps para poder soportar las aplicaciones futuras de telemedicina y mayor transferencia de información.
- El personal del proveedor portará en todo momento una identificación dentro de los sitios del Instituto durante la prestación del servicio.

D. CENTRO DE MONITOREO

El servicio incluye un centro de monitoreo, el cual controlará de forma permanente el grado, la calidad de la entrega y el soporte de los requerimientos que incluye el servicio mediante las siguientes actividades:

i. Cumplimiento de Niveles de Servicio.
ii. Mesa de Servicios.
iii. Información Ejecutiva.
iv. Repositorio de Información.

El centro de monitoreo incluye todos los recursos humanos, materiales, la metodología de entrega, soporte; manuales y procedimientos operativos necesarios para la provisión de las actividades anteriores. Cabe aclarar que las herramientas antes señaladas no necesariamente tienen que ser de la misma marca.

Requisitos técnicos del Centro de Monitoreo.

- El centro de monitoreo será accesible desde cualquier acceso vía Internet/IP por HTTP/WEB en tiempo real y a toda hora, permitiendo de igual forma realizar el seguimiento de reportes de fallas por el personal del Instituto.
- El proveedor contará con una sola herramienta de monitoreo, por lo que en caso de tener diferentes mesas de servicio (satelital y terrestre), comprobará que se cuenta con la integración correspondiente.
- Los usuarios que tendrán acceso al centro de monitoreo serán definidos en las mesas de planeación con el proveedor
- El centro de monitoreo no tendrá un límite de usuarios.
- El centro de monitoreo será provisto bajo el entorno de los siguientes estándares internacionales: ISO 20000, ISO 9001 e ISO 27001. El proveedor demostrará que cuenta con estas certificaciones y se entrega copia simple del certificado que lo comprueba.

- El centro de monitoreo tiene un nivel de servicio del 98.89% de disponibilidad mensual (ver tabla 2, Niveles de servicio) y está disponible para uso del Instituto a partir del día que entre en operación el primer sitio.
- Las herramientas del centro de monitoreo estarán alojadas en un centro de datos de alta disponibilidad y alta seguridad, mismo que deberá contar al menos con las siguientes certificaciones:
  a) ISO 9001:2008 o superior
  b) ISO/IEC 27001:2005
  c) ISO/IEC 20000-1:2011
- El centro de monitoreo se localizarse en inmuebles diferentes a los del Instituto con la redundancia correspondiente al nivel de servicio solicitado, el proveedor demostrará que el centro de monitoreo cuenta con infraestructura redundante como son acometidas eléctricas, plantas de emergencia, UPS y sistemas antiincendios. Dichas instalaciones serán visitadas por lo menos una vez al año, durante cualquier etapa de la prestación del servicio por el Instituto para su evaluación y verificar el cumplimiento de las funciones del citado centro.
- De lo anterior, el proveedor demostrará mediante manifiesto firmado por el representante legal que el centro de monitoreo cumplirá con las especificaciones solicitadas en este anexo técnico.
- El Instituto se reserva el derecho de efectuar el monitoreo del servicio de manera directa o a través de un tercero, previa firma de los "OLA's" Acuerdos Operacionales correspondientes. En su caso, el monitoreo del tercero contribuirá como una fuente de datos adicional en la determinación del cumplimiento de los niveles de servicio, así como en información complementaria para el cálculo de las deductivas y penas convencionales correspondientes, señaladas en los Términos y Condiciones.

D.i. Cumplimiento de Niveles de Servicio

El proveedor proporcionará el cumplimiento de los niveles de servicio de los servicios de comunicación, el cual será proporcionado a través de herramientas graficas especializadas y con apego a las mejores prácticas de ITIL.

El proveedor ofrece una interface de verificación de los niveles de servicio que tenga la capacidad de ser consultada en línea vía web, sin límite de usuarios, ya sea vía internet o a través de una red privada y que además cuente con indicadores gráficos de rendimiento global y por grupos de inmuebles mostrando niveles de servicios y resumen de fallas catalogadas.

El cumplimiento de niveles de servicio asimismo cumplé con los siguientes requerimientos:

- Operar los 365 días del año, los 7 días de la semana, las 24 horas del día.
- Tener un nivel de disponibilidad del 98.89% garantizado, a través de los siguientes conceptos de acuerdo con el diseño: Equipamiento de cómputo, almacenamiento y de red redundante tanto en fuentes como en procesadores.
- Contar con planta de emergencia y UPS en las instalaciones del proveedor donde se encuentre el centro de monitoreo, para garantizar la disponibilidad de la solución.
- Recolectar muestras o lecturas de indicadores de rendimiento diarias.
- Capacidad de medir en línea y en tiempo real el comportamiento operativo de los componentes de comunicaciones de la solución. El comportamiento operativo versará sobre los componentes como el CPU, memoria, ancho de banda de los equipos de telecomunicaciones.
- Incluye una herramienta de generación de reportes en línea para la toma de decisiones relacionadas con el tráfico de la red, niveles de servicio e indicadores de rendimiento de la red.
- Los indicadores de rendimiento son enfocados a los equipos de telecomunicaciones de los cuales se pude extraer información del CPU, memoria, ancho de banda latencia y paquetes perdidos.
- Considera alarmas interactivas para cualquier evento que rebase los umbrales definidos en las mesas de planeación con el proveedor y que pongan en riesgo la operación de la red objeto del servicio con aviso vía SMS y/o correo electrónico, tanto para personal del Instituto como para personal del proveedor, quien tendrá la responsabilidad de atender de manera oportuna los incidentes con la finalidad de cumplir

con los niveles de servicio solicitados en el presente anexo técnico. Los avisos al personal del Instituto se definirán de manera conjunta con el proveedor en las mesas de planeación.

- Generar información y reportes para la planeación de capacidades de los servicios de comunicación de acuerdo a lo solicitado por el Instituto en las mesas de planeación.
- Manejar vistas completas con un sistema visual de alarmas representando en forma gráfica al menos los siguientes indicadores de niveles de servicio:
    - Disponibilidad de servicio por sitio y por equipo.
    - Latencia por sitio.
    - Pérdida de paquetes por sitio.
    - Paquetes con error de trama por sitio.
    - Consumos de instancias de procesador, memoria y cualquier otro indicador permitido por el tipo de MIB (Management Information Base).
    - Consumo de ancho de banda por sitio.
    - Medir el comportamiento del tráfico clasificado por clase de servicio monitoreando, retardos, disponibilidad, paquetes perdidos por cada enlace.

El proveedor será responsable de realizar los estudios de desempeño de la red y de las capacidades diarias a través de la medición del tráfico generado de entrada y salida y de la utilización de los equipos activos de comunicaciones, por lo que contará con herramientas que permitan generar, verificar y almacenar estadísticas del desempeño, capacidad y utilización de los componentes de soporte del servicio.

Los registros generados en el proceso de verificación de los niveles serán utilizados para apoyar al Instituto en el proceso de validación de los niveles de servicio que se contratarán con el proveedor.

Será capaz de gestionar los centros de costos por cada sito del Instituto, es decir llevar a cabo el análisis de desempeño de la red y de las capacidades diarias a través de la medición del tráfico generado de entrada y salida, así como de la utilización de los equipos de comunicaciones por cada sitio.

D.ii. Mesa de Servicios

El servicio a través del centro de monitoreo incluye una mesa de servicios que será el único punto de contacto para la atención de los usuarios del Instituto y del tercero que el IMSS defina para la vigilancia del cumplimiento de los niveles de servicio.

La mesa de servicios del proveedor será la responsable de detectar, comunicar y reparar cualquier falla de los servicios de comunicación, en tiempo y forma para poder cumplir con los niveles de servicios establecidos en este anexo técnico.

El proveedor presentará los procedimientos probados y procesos certificados ISO 9001, ISO 20000 e ISO 27001 que actualmente utiliza en los siguientes puntos que a la vez serán su responsabilidad el dar cumplimiento durante la vigencia del contrato:

- Registro y escalación de los reportes de falla y de requerimientos que usará para la operación del servicio, considerando que deberán ser atendidos por un operador, el cual se encargará de darle seguimiento y solución en su caso hasta el cierre definitivo del reporte, ya sea mediante soporte a primer nivel como de escalación a terceros.
- Recepción en primera instancia de los reportes de incidentes detectados por el Instituto y/o del tercero que el IMSS defina para la vigilancia del cumplimiento de los niveles de servicio en forma reactiva, es decir aquellas fallas que no fueron detectadas de manera oportuna.
- Coordinación de uno o más proveedores que se encuentren involucrados en la prestación del servicio en un determinado incidente.
- Conteo de los tiempos de inicio y término de los incidentes.

- Revisión con el Instituto y/o del tercero que el IMSS defina para la vigilancia del cumplimiento de los niveles de servicio, que las funcionalidades del servicio se encuentren operando completamente después de un incidente.
- De acuerdo a las mejores prácticas, se realizará el almacenamiento en una base de datos de la información correspondiente al proceso de resolución de incidentes.
- Notificación al Grupo Administrador del Contrato, desde el inicio hasta la finalización de un evento de falla vía los siguientes medios posibles: correo electrónico, vía telefónica, envío de mensajes SMS, notificador de la herramienta de mesa de servicios.
- Entregar al Grupo Administrador del Contrato con una periodicidad mensual, un reporte de los incidentes, sus tiempos de atención y caídas de los enlaces.

el proveedor entregará como parte de su propuesta técnica, el modelo que utiliza para el manejo de los diferentes perfiles que intervienen en sus procesos y la organización de su mesa de servicios, lo anterior, de forma enunciativa y no limitativa:

- Matriz de escalación: el proveedor entregará en su propuesta técnica el modelo de matriz de escalación que utilizará en caso de resultar adjudicado para controlar los servicios de conectividad que recibirá el Instituto durante la vigencia del contrato.
- El proceso de atención a incidentes: La mesa de servicios deberá incluir los campos necesarios para la óptima clasificación y almacenamiento de los reportes que serán acordados junto con el Instituto y estos deberán apegarse a las mejores prácticas como los KPI de ITIL.

el proveedor presentará en la propuesta técnica la metodología, formatos y procedimientos que usará para medir en forma mensual la satisfacción del servicio que recibe el Instituto y deberá mostrar las estrategias que llevará a cabo para lograr un proceso de mejora continua.

D.iii. Información Ejecutiva

El proveedor además de entregar en forma periódica o a petición expresa por parte del Instituto, los reportes electrónicos de los resultados de su actividad; contará con información ejecutiva a través de un portal en Internet, basado en la administración de indicadores claves de desempeño.

La información ejecutiva proporcionará la facilidad de realizar consultas personalizadas de la información generada global y por sitio, así como sus combinaciones y permitir su importación a formato electrónico e impresión en forma local.

A través del portal, permitirá consultas simultáneas de múltiples usuarios. El formato detallado de la información se definirá, en reunión de trabajo como máximo treinta días hábiles después de la notificación de fallo.

El portal, al menos, presentará en tiempo real y de manera sencilla la interpretación de las variables monitoreadas, tales como: porcentajes de tráfico de diferentes clases vs prioridad de los sitios, reporteo por sitio por tipo de paquete, los cuales combinarán variables de SLA (latencia, jitter, perdida de paquetes, etc.) por cada grupo de prioridad de sitios y asociarlo a su precio mensual. Para lo anterior, el sistema y la arquitectura queda a consideración del proveedor

Asimismo, los reportes tendrán la capacidad de entregar la siguiente información:

- Usuarios que reportan incidencias.
- Reparaciones realizadas (y tiempo invertido en las reparaciones).
- Número de atenciones telefónicas realizadas durante el año o periodo especifico.
- Disponibilidad física de equipos y medios.
- Niveles de servicio.
- Tipo de tráfico por puertos y protocolos.

- Retardo/Latencia.
- Reportes de dispositivo específicos por nodo del servicio.
- Los reportes deberán permitir seleccionar el periodo (por día, semana, mes, año, de fecha a fecha) y/o por grupo de nodos.
- Reportes de utilización del ancho de banda de salida y entrada
- Reportes de tendencias, por tendencia se deberá entender a las proyecciones del comportamiento de la red con base en su comportamiento histórico.
- Proveer en forma mensual estadísticas de las incidencias.
- Caídas de los enlaces y su duración por sitio y globales.

D.iv. Repositorio de Información

Será responsabilidad del proveedor proporcionar al Instituto un repositorio de información que cumpla con las siguientes funcionalidades.

El proveedor será responsable de contar con herramientas y procedimientos que garanticen la continuidad, seguridad e integridad de la información almacenada durante la vigencia del contrato.

La información por sitio será almacenada en forma centralizada durante la vigencia del contrato en un repositorio físico de información, con capacidad de almacenamiento suficiente, en las instalaciones del proveedor que cuenta con:

- Métricas de los SLA.
- Mantenimientos correctivos.
- Administración de cambios. Entendiéndose como administración de cambios al proceso basado en ITIL o ISO 20000 que tiene la finalidad de controlar el ciclo de vida de todos los cambios y teniendo como objetivo principal viabilizar los cambios beneficiosos con un mínimo de interrupciones en la prestación de servicios de TI.
- Base de datos de configuraciones. Por base de datos de configuraciones se deberá entender como una base de datos que contiene detalles relevantes de cada elemento de configuración y de la relación entre las mismas, incluyendo equipo físico, software y la relación entre incidencias, problemas, cambios y otros datos del servicio.
- Base de datos de capacidades.
- Base de datos de problemas.
- Reportes de monitoreo de indicadores y niveles de servicio.
- Reportes de la mesa de servicios.
- Respaldos de configuraciones de Servidores y equipos CPE (Client Premises Equipment).
- Memoria técnica.
- Incidentes.
- Análisis de tendencias.
- Plan de mejora de servicios.

La plataforma cumplirá con las siguientes funcionalidades:
Capacidad de dar seguimiento a los documentos e impedir que alguien pueda sobre-escribirlos, así como guardar una versión de cada documento en el que se hayan introducido cambios.

La información generada podrá ser consultada en el momento que el Instituto así lo considere necesario durante la vigencia del contrato, se contará con la capacidad de realizar consultas históricas y respaldos de las muestras tomadas por cada sitio en medios magnéticos u ópticos.

La información de las muestras tomadas por sitio, reportes, documentos y demás productos que resulten de las actividades realizadas por el centro de monitoreo serán propiedad exclusiva del Instituto.

Al finalizar la vigencia del contrato, en un plazo no mayor a 2 meses, el proveedor entregará en medios ópticos al Instituto toda la información que haya sido generada, así como eliminar la misma de sus equipos e instalaciones. El proveedor se compromete a guardar la confidencialidad de la información del Instituto generada en sus equipos durante la vigencia del contrato y de no divulgarla y hacer un mal uso de esta.

PARTIDA 2

Operbes S.A. de C.V. participa en la prestación del servicio objeto del presente contrato que se prestará como continuidad al contrato DC17S0082 y su Convenio Modificatorio No.1, a partir del día siguiente a la notificación de adjudicación y hasta el 31 de diciembre de 2020, con el proveedor que actualmente presta los servicios en el contrato DC17S0082 y su Convenio Modificatorio No.1.

7.2. Servicio Administrado de Acceso a Internet

Operbes S.A. de C.V. proporcionará el servicio de acceso a la red de Internet, para los nodos o inmuebles identificados en el Apéndice 2, sección en donde se define la capacidad requerida para cada uno de los nodos en cuestión. El servicio de acceso a Internet deberá proporcionarse conforme a los niveles de servicio establecidos en el presente documento.

El alcance de los servicios suministrados por Operbes S.A. de C.V. incluirá funcionalidades y servicios administrados de seguridad en cada uno de los 3 nodos listados en el Apéndice 2 "Inventario de Servicios de Acceso a Internet", mismos que con excepción del atributo de "Clean Pipes" (Capacidad de Mitigación de Ataques de Negación de Servicio) que estará integrado a cualquier Servicio de Acceso a Internet en los 3 nodos, serán cotizados de manera desagregada al servicio administrado de acceso a Internet (medio y acceso), tal y como se observa en el Catálogo de Servicios de este Anexo Técnico y en la Sección I "Precios Unitarios". Estas funcionalidades y servicios administrados de seguridad se describen más adelante en este anexo técnico.

Se complementará la mitigación en la nube con la protección anti-DDoS en sitio para los portales web descritos en el anexo, incluyendo todos los elementos para la protección Web de los portales descritos en el anexo.

Debido a la importancia y criticidad de los Servicios Administrados de Acceso a Internet, éste tendrá las siguientes características mínimas:

- Para tráfico hacia o desde el Instituto y con destino a una red o servicio dentro del Territorio Nacional se privilegiará el intercambio de tráfico en el IXP o por medio de acuerdos (peering) entre operadores nacionales a fin de que el tráfico generado en México permanezca en el territorio nacional.
- Operbes S.A. de C.V. contará con acuerdos de interconexión globales (públicos y privados), los cuales faciliten el acceso a las aplicaciones y servicios digitales del IMSS
- Operbes S.A. de C.V. ofrecerá la mejor ruta y balanceo de carga inteligente basado en la utilización del enlace para mejorar el rendimiento y disponibilidad de las aplicaciones o servicios digitales que el IMSS considere críticos

El servicio a Internet contará con un enlace alterno, que presente diversidad de acceso y de ruta en su red dorsal, así como la infraestructura necesaria para realizar la transferencia en caso de falla al enlace redundante desde el enlace activo (descritos en el Apéndice 2), permitiendo el acceso a las aplicaciones o servicios digitales del IMSS sin realizar cambio en el direccionamiento IP. Este enlace alterno deberá ser de infraestructura propiedad de Operbes S.A. de C.V..

Ambos enlaces de acceso a Internet (primario y alterno) formarán parte del backbone de Operbes S.A. de C.V. de la partida 2, y estos enlaces deberán estar conectados hacia dos puntos diferentes del backbone de Internet de Operbes S.A. de C.V.

El IMSS cuenta actualmente con un segmento homologado de direcciones IP, por lo que es importante mencionar que los servicios que se tienen hoy en día están montados en el segmento antes mencionado. Inicialmente, Operbes S.A. de C.V. proporcionará un bloque de 256 direcciones IP homologadas para el IMSS.

Este requerimiento, permitirá, cuando así sea solicitado por el IMSS, el incremento en bloques de 256 direcciones de IP homologadas sin generar costos adicionales.

El servicio de acceso a Internet será ofertado en un esquema en demanda, partiendo de un "piso" mínimo y con un "techo" máximo al cual se puede acceder con sucesivas ampliaciones con incrementales fijos y a precio unitario definido de acuerdo con el Catálogo de Servicios de esta contratación. El servicio será facturado y pagado por el IMSS con las características especificadas más adelante y de acuerdo con los rubros de servicio definidos en la Sección I "Precios Unitarios".

7.2.1. Requisitos Generales

Operbes S.A. de C.V. proporcionará al IMSS el acceso a Internet cumpliendo los siguientes requerimientos, algunos de ellos ya introducidos en la sección anterior:

- Operbes S.A. de C.V. demostrará, como parte de su Propuesta Técnica, que cuenta con enlaces de al menos un equivalente de 5 Gbps hacia el backbone de Internet y estas conexiones estarán en diferentes POP's, los cuales deben ser parte integral de la red de Operbes S.A. de C.V. y no de un tercero.
- Operbes S.A. de C.V. contará con acuerdos de interconexión globales (públicos y privados), los cuales deberán facilitar el acceso a las aplicaciones y servicios digitales del IMSS. Además de esto, Operbes S.A. de C.V. manifestará por escrito, como parte de su Propuesta Técnica, que cuenta con "Acuerdos de Intercambio" en el punto de intercambio de tráfico de Internet con por lo menos tres proveedores nacionales (y mencionar en el documento cuáles son estos proveedores)
- Operbes S.A. de C.V. integrará, como parte de su Propuesta Técnica, copia de documentación en la que comprueben los "Acuerdos de Intercambio con por lo menos tres proveedores nacionales.
- Operbes S.A. de C.V. integrará, como parte de su Propuesta Técnica, un diagrama genérico de su red de Internet. En el diagrama se deberán indicar las conexiones que se tienen hacia el punto de intercambio de tráfico de Internet, así como su capacidad.
- Operbes S.A. de C.V. especificará, como parte de su Propuesta Técnica, que el medio para la entrega del servicio y la última milla serán con fibra óptica y se adjunta un mapa del trayecto de la fibra desde el IMSS hasta el nodo del acceso a Internet.
- Operbes S.A. de C.V. ofertará, dentro de sus Propuestas Técnica y Económica, un acceso a Internet mediante enlaces de acceso en demanda con su respectiva redundancia, con la posibilidad de manejar anchos de banda mayores a 1 Gbps, usando una red de servicio metro ethernet para el acceso punto a punto, el cual deberá ser exclusivo para el IMSS, y no deberá ser multiplexado con otros servicios, teniendo como puntas de enlace para los enlaces activos y pasivos, Centros de Datos que prestan servicios al IMSS, de acuerdo a lo especificado en el Apéndice 2

Proporcionar un direccionamiento completo clase C portable para el IMSS, soportando el protocolo BGP4 (Border Gateway Protocol).

7.2.1.1. Acceso a Internet Bajo Demanda

Las ubicaciones de los servicios de acceso a internet se detallan en el apéndice 2 del presente documento.

El Servicio Administrado de Acceso a Internet, como se ha mencionado, forma parte de la partida 2 de este ejercicio de contratación. El servicio en cuestión será facturado en demanda de acuerdo con el ancho de banda solicitado por el Instituto bajo el siguiente procedimiento de cálculo:

- Operbes S.A. de C.V. cobrará el ancho de banda base, más los incrementales (de 10 MB) que apliquen. En caso de que los incrementales hayan sido solicitados durante el transcurso del mes, los

incrementales se cobrarán de manera proporcional a los días devengados del mes, considerando meses de 30 días.

- Operbes S.A. de C.V. realizará el monitoreo diario del uso del circuito con poleos cada 5 minutos, tanto del tráfico de entrada como el de salida, para un total de 288 muestras de tráfico de entrada y otras 288 muestras de tráfico de salida.
- Se ordenarán las 288 muestras de entrada de manera decreciente, al igual se deberán de ordenar las 288 muestras de salida de manera decreciente.
- Se eliminará el 5% de las muestras mayores de entrada y el 5% de las muestras mayores de salida.
- Después de eliminar el 5% de ambas muestras (entrada y salida) se tomará la muestra mayor como muestra representativa del consumo del ancho de banda (Mbps) de dicho día.
- El mismo procedimiento se realizará diariamente
- El servicio en cuestión será facturado en demanda de acuerdo al ancho de banda solicitado por el instituto bajo el siguiente procedimiento de cálculo: Operbes S.A. de C.V. cobrará el ancho de banda base, más los incrementales (de 10 MB) que apliquen. En caso de que los incrementales hayan sido solicitados durante el trascurso del mes, los incrementales se cobrarán de manera proporcional a los días devengados del mes, considerando meses de 30 días.
- El cobro total se compondrá de la suma de las 30 lecturas diarias, con base mensual, con un consumo mínimo y un costo por cada 10 Mbps adicionales de acuerdo con la siguiente tabla:

Nodo de Internet	Inmueble	Piso (consumo mínimo garantizado)	Techo (consumo máximo)	Redundancia	Requerimientos Especiales	Usuarios o Consumidores aproximados (cifra referencial)
Nube IMSS Digital	Centro de Datos donde se aloja la "Nube IMSS Digital"	310 Mbps	1 Gbps	SI	Direcciones IP homologadas (no portables) que se requieran	Al menos 120,000 usuarios del IMSS
CeNaTi Nuevo León	CeNaTi Monterrey	155 Mbps	1 Gbps	SI	256 direcciones IP homologadas (no portables)	Al menos 256 servidores
CeNaTi México D.F.	CeNaTi México D.F.	32 Mbps	155 Mbps	SI	Direcciones IP homologadas (no portables) que se requieran	Al menos 20,000 usuarios del IMSS

El dominio que Operbes S.A. de C.V. manejará dentro de la solución es el asignado al IMSS (imss.gob.mx) con un DNS activo en Internet administrado por Operbes S.A. de C.V..

Operbes S.A. de C.V. garantizará una disponibilidad mínima del servicio del 99.98% de cada par de enlaces (dado que los 3 nodos son redundantes) de manera mensual en su backbone de conexión a Internet, así como los enlaces de última milla.

Gestión de Fallas especializada 7x24x365 con la certificación ISO 9002 o ISO 9001:2000 o ISO 20000 en cualquiera de sus versiones para brindar el máximo servicio (Centro de Atención de Fallas de Operbes S.A. de C.V.)

Contará y proporcionará acceso a las personas que designe el IMSS a las siguientes aplicaciones en línea y que operen en tiempo real para verificar y garantizar el desempeño de la red:

- Estadísticas gráficas de tráfico, utilización del circuito de Entrada/Salida (IN/ OUT)
- Operbes S.A. de C.V. incluirá el cableado hasta el equipo de comunicaciones del IMSS a través de puertos Gigabit Ethernet en fibra óptica y donde se necesite a 10/100/1000 Mbps, el cual será su responsabilidad durante la duración del servicio, así como el switch de acceso que forme parte del servicio propuesto. El punto físico de demarcación del servicio será el puerto físico del equipo de

comunicaciones del IMSS en los nodos especificados. Se deberán brindar 2 puertos de 1GE Óptico (multimodo) y 2 puertos de cobre 10/100/1000.

En la propuesta técnica, Operbes S.A. de C.V. menciona que entregará el servicio en fibra óptica, nombre de la empresa que proporcionará la última milla y un mapa del trayecto de la fibra desde los nodos del IMSS especificados en el Apéndice 2, hasta el nodo de Operbes S.A. de C.V. del acceso a Internet.

7.2.1.2. Arquitectura del Servicio

El servicio de acceso a Internet será utilizado por dos tipos de usuarios, el interno del IMSS (funcionario) y el externo (ciudadano). El externo normalmente utilizará este servicio al ingresar a las paginas institucionales del IMSS, para la realización de algún trámite o consulta institucional; el usuario interno del IMSS necesita de este servicio para la transacción de información con otras instituciones, ya sea gubernamentales, de salud o bancarias, o para comunicarse con el derechohabiente para la realización de un trámite con la institución, por mencionar solo algunas de las funciones.

Operbes S.A. de C.V. ofrecerá al IMSS un servicio de Internet de las siguientes características, para cada uno de los enlaces activos definidos en el Apéndice 2:

- Internet bajo demanda con posibilidad de transferencia (velocidad) "piso" de 310, 155 y 32 Mbps, respectivamente, de acuerdo con la tabla anterior especificada en la sección "Acceso a Internet Bajo Demanda"
- Alta disponibilidad del servicio con posibilidad de uso de protocolo HSRP en equipo CPE
- Servicio de mitigación de Ataques de Denegación de Servicio Distribuido (DDoS Clean Pipes, como es conocido en idioma inglés)
- Servicio de Balanceo vía BGP

Operbes S.A. de C.V. ofrecerá conectividad a Internet utilizando infraestructura de red Metro Ethernet, entregando una conexión punto-a-punto o punto extendida a lo largo de la red de Operbes S.A. de C.V. hacia los puntos de demarcación. Se definirá una VLAN para el servicio de Internet.

Punto de Demarcación:

Los Servicios Administrados de Acceso a Internet que se entregarán en los tres Nodos Centrales de la Institución, considerarán que éstos cuentan con distintos niveles y tipos de Infraestructura frontera, a la que habría que conectar la infraestructura propia de Operbes S.A. de C.V. para poder ofrecer los servicios solicitados.

Operbes S.A. de C.V. considera, como parte de las propuestas y económicas, toda la infraestructura, licenciamiento, cableado, servicios de soporte técnico, garantías extendidas, mantenimiento, operación, además de toda la infraestructura habilitadora y red de telecomunicaciones requeridas, y que permitan brindar el Servicio de Internet con las siguientes características:

- Servicio de Internet dedicado, entregado a través de infraestructura propiedad de Operbes S.A. de C.V. en enlaces Ethernet con interfaces de 1 Gbps, de acuerdo a la infraestructura de frontera exhibida para cada nodo en la sección "Perfil para Centro de Datos". Los servicios de conectividad solicitados contarán con mecanismos de redundancia en todos los elementos activos y pasivos usados para transportar y brindar conectividad a los enlaces solicitados. Para dar cabal cumplimiento a la solicitud de redundancia para cada uno de los nodos solicitados, Operbes S.A. de C.V. incluye en la propuesta técnica que cada nodo deberá recibir el servicio con las siguientes características de conectividad:
- Enlaces redundantes en configuración activo-activo. El tráfico de cada Nodo deberá estar balanceado entre los dos enlaces en configuración activo-activo, y la medición de ancho de banda del nodo será el resultante de la suma del tráfico en ambos. Los enlaces redundantes deberán estar configurados para permitir el transporte del ancho de banda solicitado en el nodo, a pesar de que uno de los enlaces esté fuera de servicio. Es importante aclarar que el ancho de banda solicitado para cada nodo se compone de la suma resultante del "piso" de ancho de banda solicitado inicialmente, más todos los incrementos

de ancho de banda consumidos en dicho momento para dicho nodo, a través del "Servicio de Incremento de Ancho de Banda para Internet" de este Anexo Técnico.

- Equipos de transporte de "última milla" en las terminales de los sitios del IMSS en cada Centro de Datos, donde la infraestructura sea completamente redundante en todos sus componentes activos, tal como: Fuentes de Poder redundantes, tarjetas de enlaces de fibra, tarjetas controladoras y/o procesadoras, etc.
- Equipos de Ruteo redundante. En los Nodos donde se requiere que Operbes S.A. de C.V. entregue el Servicio de Internet, a través de ruteadores, éstos serán redundantes y el servicio deberá incluir al menos dos ruteadores en cada nodo central. Los enlaces redundantes, deberán interconectarse uno a cada ruteador. Adicionalmente, la configuración de los equipos deberá considerar la existencia del ruteador redundante, de tal forma que, en el evento de la caída de uno de los ruteadores, o los enlaces de Internet mismo, todas las funciones y tráfico del nodo sean completamente absorbidos por el equipo sobreviviente al evento. Esta transición de redundancia sucederá de manera automática e inmediata ante la caída, y deberá reestablecerse a su condición de operación normal, una vez que el ruteador y enlace fallido se reestablezca. La configuración de los equipos, enlaces y protocolos de ruteo deberá hacerse de tal forma que permita cumplir y/o exceder los Niveles de Servicio solicitados por el IMSS.
  La redundancia que se solicita se refiere a un esquema de N+1 en toda la solución del nodo nube IMSS digital.
  Se brindan 2 puertos de 1GE Óptico (multimodo) y 2 puertos de cobre 10/100/1000.
- Enlaces de red Ethernet entre los equipos de frontera detallados en la sección "Perfil para Centro de Datos" y los equipos de ruteo de Operbes S.A. de C.V., y/o equipo de transporte de última milla aquí descritos. Los enlaces Ethernet deberán ofrecerse en fibra óptica, y deberán considerar el tipo de fibra óptica y conectores específicos de cada nodo, debiendo ser dichos enlaces infraestructura propiedad de Operbes S.A. de C.V.

Es importante aclarar que Operbes S.A. de C.V. incluye todos estos requerimientos como parte de los Servicios Administrados de Acceso a Internet, y que el IMSS no incurrirá en ningún costo adicional al detallado en el Catálogo de Servicios y en la Sección I: Precios Unitarios.

Ancho de Banda:
El Ancho de Banda del servicio será configurable en demanda desde un piso de 310, 155 y 32 Mbps, de acuerdo con la tabla especificada en la sección "Acceso a Internet Bajo Demanda" y con incrementos (paquetes de cobro por consumo mensual) de 10 Mbps, hasta llegar a un máximo de 1 Gbps, tal como se indica en la tabla anterior.

Tráfico:
El tráfico de LAN transportado en la red Metro Ethernet recibirá tratamiento de capa 3 hacia los equipos que proporcionan la salida a Internet de Operbes S.A. de C.V.

Los anuncios de las redes del IMSS serán realizados por el (los) equipo(s) de Operbes S.A. de C.V., respetando todas las políticas de anuncios que tienen el resto de los equipos de la red de Internet.

Los servicios Ethernet ofrecidos podrán ser limitados en su ancho de banda dentro de las capacidades físicas de las interfaces ópticas o eléctricas en las que se entreguen, de tal forma que se puedan tener techos máximos de consumo ajustables en los intervalos solicitados por el IMSS.

Multi-homming:
El IMSS requiere un servicio de Internet que pueda ser parte de una arquitectura multi-homming donde se tenga una convivencia del servicio con dos o más proveedores de servicio de Internet (ISP), bajo un sistema que permita la manipulación de tráfico y distribución de cargas por medio del protocolo de enrutamiento BGP4 (Border Gateway Protocol). Por lo anterior, Operbes S.A. de C.V. considerará la posibilidad de enlazar el CPE que provea con su solución, con el CPE del proveedor de Internet ISP alterno vía el protocolo I-BGP-4 para el

manejo adecuado de todos los criterios y métricas disponibles y posibles del mismo protocolo para configurar en este tipo de ambientes.

Servicio de Balanceo vía BGP:
Operbes S.A. de C.V. integrará un sistema completo y automatizado de balanceo de carga vía BGP, mismo que deberá interactuar con los CPEs provistos por Operbes S.A. de C.V., así como con los provistos por el ISP alterno de Internet.

Disponibilidad:
El IMSS requiere de una disponibilidad, en ambos servicios, del 99.98% en su backbone de conexión hacia Internet. Para el caso del enlace de última milla, se deberá garantizar un valor de disponibilidad de 99.98%.

Monitoreo y Reportes:
Operbes S.A. de C.V. proporcionará una herramienta, basada en Web, que permita obtener reportes de desempeño del servicio hacia Internet.

Los formatos de los reportes y la frecuencia de entrega se elaborarán de común acuerdo entre el IMSS y Operbes S.A. de C.V. Dichos reportes podrán ser exportados a formatos tales como HTML, PDF, ASCII y Excel.

7.2.1.3. **Componentes Habilitadores para Internet**
Para el caso de nuevos requerimientos, a continuación, se enlistan los requisitos y funcionalidades mínimas que deberán cumplir los equipo CPE para el Servicio Administrado de Acceso a Internet, de acuerdo con la arquitectura previamente definida:

- Operbes S.A. de C.V. proporcionará equipos CPE's (Customer Premise Equipment), para recibir en los sitios especificados en el Apéndice 2, los enlaces de comunicaciones del servicio de Internet.
- Operbes S.A. de C.V. proporcionará la infraestructura y red de telecomunicaciones y enlaces para Internet.
- Operbes S.A. de C.V. proveerá al IMSS acceso de tipo "lectura" a la configuración de cualquier equipo CPE que incluya con la solución y, a su vez, deberá homologar las configuraciones de sus equipos CPE con los del ISP alterno descrito en la arquitectura del servicio. El IMSS podrá en todo momento revisar las configuraciones de los equipos y participar en el establecimiento de los Acuerdos de Nivel de Operación (OLAs) entre los distintos ISPs.
- Con el fin de contar con un servicio homogéneo a nivel nacional, los equipos CPE's deberán cumplir con el modelo y las características mínimas descritas más adelante.
- Operbes S.A. de C.V. incluye en su Propuesta Técnica un listado de los equipos que integran su solución, junto con diagramas con el diseño propuesto, en los que se identifique en forma clara y detallada el apego a la arquitectura y a la topología aquí descrita.

- Operbes S.A. de C.V. es responsable de:
  - La continuidad del servicio en los nodos o inmuebles especificados por el IMSS en el Apéndice 2
  - La configuración lógica y física de los equipos CPE's
  - La configuración del equipamiento sitio por sitio, con base en el diseño basado en la arquitectura descrita en este documento, y en la ingeniería de Operbes S.A. de C.V.
  - El mantenimiento correctivo del equipo
  - El respaldo y reposición de equipo en caso de falla, incorporando un equipo de iguales o mayores capacidades
  - Los traslados y horas-ingeniero para las actividades mencionadas anteriormente
  - La creación de los perfiles de la red del cliente en las plataformas de administración
  - Las pruebas de turn-up de la red punta a punta
  - La realización de altas, bajas, cambios y movimientos lógicos

Descripción de alto nivel de los componentes habilitadores:

- CPE de Internet
  - Contará con la suficiente capacidad en hardware para soportar el procesamiento de todo el tráfico que el IMSS demande en su servicio de Internet, conformado por un par de equipos switch/router capa 3 del modelo de la OSI, con el máximo de memoria y procesador de alto desempeño.
  - Tendrá las posibilidades de recibir la tabla completa de rutas del Internet, enrutar usando protocolos como OSPF, BGP, Estático.
  - Proveerá capacidades de conmutación a nivel 2 y 3 de la OSI de alto desempeño, que sirva de distribución del servicio de Internet hacia el interior de la infraestructura del IMSS. Aquí se podrán aplicar, de manera enunciativa más no limitativa, el manejo óptimo de políticas de enrutamiento internas y externas, listas de acceso, QoS, entre otros.
  - Contará con conexiones 10/100/1000 y conexiones 1 GE óptico.

7.2.1.4. **Servicios de Seguridad para el Nodo "Nube IMSS Digital"**

En virtud de que el IMSS se encuentra consolidando la plataforma que le permitirá el alojamiento de servicios digitales de nueva generación, en el Centro de Datos que le presta servicios bajo el concepto "Nube IMSS Digital", la mayor parte de las funcionalidades de seguridad en sitio que serán aplicadas al tráfico de Internet, serán provistas por el IMSS dentro de esta plataforma. Por esta razón, Operbes S.A. de C.V. únicamente entregará el tráfico de Internet atendiendo al punto de demarcación descrito en la "Arquitectura del Servicio" y entregando dicho tráfico a la plataforma mencionada, sin perder de vista los atributos de "Clean Pipes" (Capacidad de Mitigación de Ataques de Negación de Servicio) y los mencionados previamente, para darle al IMSS garantía de limpieza de los datos en dichos aspectos. **Es por ello que únicamente existe un elemento en el Catálogo de Servicios, denominado "Servicios Administrados de Acceso a Internet para Nodo "Nube IMSS Digital", que cubre la totalidad de servicios requeridos en este nodo, de manera mensual.**

7.2.1.5. **Servicios de Seguridad para el Nodo "Monterrey"**

Para el caso del Servicio Administrado de Acceso a Internet entregado en el Nodo CeNaTi Monterrey, listado con mayores detalles respecto de su ubicación en el Apéndice 2, Operbes S.A. de C.V. proporcionará servicios de seguridad asociados con el tráfico de Internet a ser consumido por el IMSS.

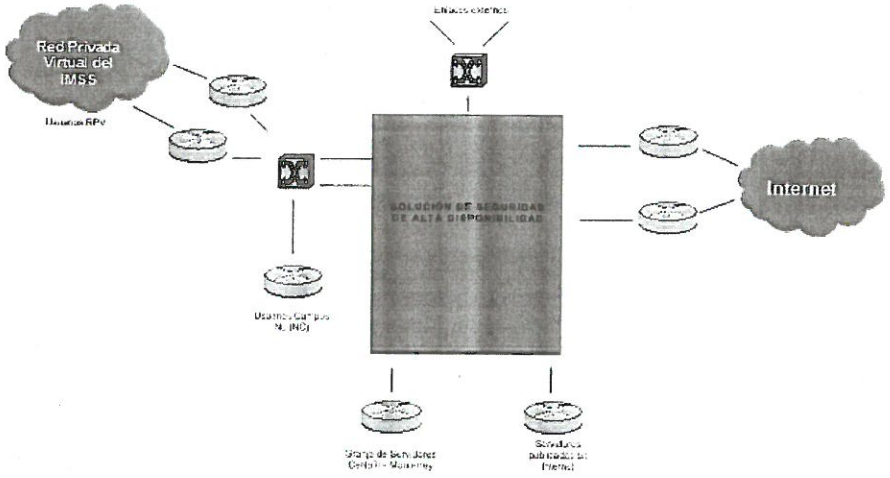
Operbes S.A. de C.V. **considerará, para este nodo, los costos de estos servicios de manera desagregada (separada) del Precio Unitario Mensual correspondiente a este acceso a Internet dentro del Catálogo de Servicios, con excepción del servicio de Clean Pipes (Capacidad de Mitigación de Ataques de Negación de Servicio), mismo que se considera integrado al Precio Unitario Mensual del Acceso a Internet.** Toda la infraestructura de hardware y software que Operbes S.A. de C.V. incorpore para cumplir con estos requisitos deberá ser nueva y de uso exclusivo para el IMSS, no usada ni reconstruida.

De manera enunciativa más no limitativa, los requerimientos técnicos del IMSS en este sentido para con Operbes S.A. de C.V. son:

- Administrar la solución de seguridad propuesta para cumplir los requerimientos funcionales descritos. Adicionalmente, proporcionará en las instalaciones del IMSS (en la ciudad de México) un sistema de supervisión para todos los elementos de la solución, similar a la que encuentre operando como parte de la solución de Operbes S.A. de C.V., para la comprobación de las funcionalidades requeridas por el IMSS y que cuente con la capacidad de al menos 10 usuarios concurrentes.
- Poner en operación la solución localizada de seguridad basándose en las políticas operativas existentes en el ambiente de seguridad actual, mismas que serán compartidas por el Grupo Administrador del Contrato a Operbes S.A. de C.V. durante mesas de trabajo. Se realizará un análisis de vulnerabilidades sobre la infraestructura de red en el CeNaTi - Monterrey y sobre la propia solución de seguridad, a fin de que se identifiquen los aspectos de vulnerabilidad en la seguridad de la infraestructura del IMSS
- Proporcionar un esquema de replicación inmediata de las modificaciones en las políticas de los

diferentes elementos y dispositivos que conformen la solución de seguridad específica para el Nodo CeNaTi Monterrey.

Operbes S.A. de C.V. incluirá el hardware y/o software necesario para proporcionar al menos las siguientes funcionalidades tomando el diagrama como referencia:



- Solución en Alta Disponibilidad de Prevención de intrusos (IPS), que apoye a asegurar los servicios publicados por el IMSS y red interna Institucional y que soporte al menos 120,000 usuarios concurrentes)
- Solución en Alta Disponibilidad de Firewall, que soporte al menos 120,000 usuarios concurrentes
- Solución en Alta Disponibilidad de análisis de flujo con capacidad de detección de anomalías en tráfico
- Solución de Mitigación de Ataque de Negación de Servicios

El canal de comunicación y capacidad de procesamiento de cada elemento en la solución de seguridad debe estar dimensionado con una política de al menos cuatro veces mayor al respectivo enlace a Internet, dependiendo del origen/destino de la información.

7.2.1.6. **Servicios de Seguridad para el Nodo "D.F."**
Para el caso del Servicio Administrado de Acceso a Internet entregado en el Nodo CeNaTi D.F., listado con mayores detalles respecto de su ubicación en el Apéndice 2, Operbes S.A. de C.V. proporcionará servicios de seguridad asociados con el tráfico de Internet a ser consumido por el IMSS.

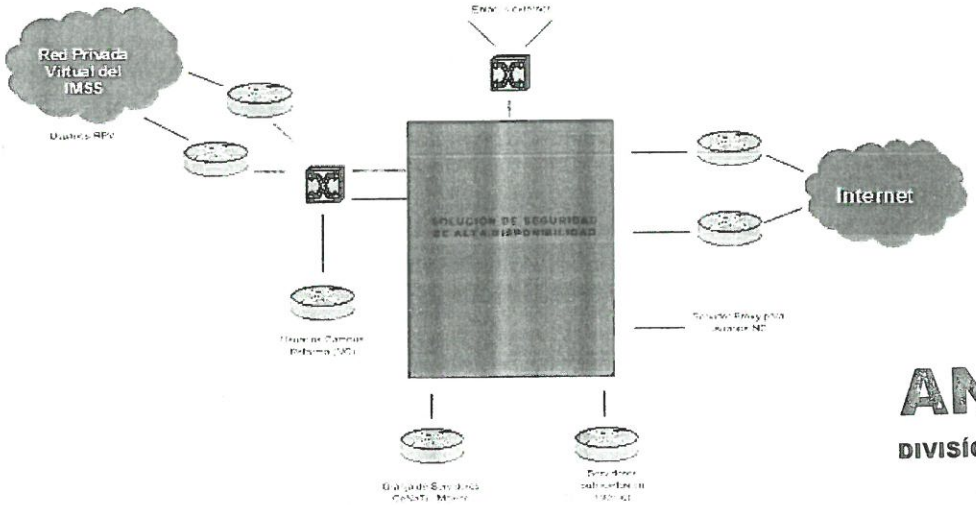
Operbes S.A. de C.V. **incluirá, para este nodo, los costos de estos servicios de manera desagregada (separada) del Precio Unitario Mensual correspondiente a este acceso a Internet dentro del Catálogo de Servicios, con excepción del servicio de Clean Pipes (Capacidad de Mitigación de Ataques de Negación de Servicio), mismo que se considera integrado al Precio Unitario Mensual del Acceso a Internet.** Toda la infraestructura de hardware y software que Operbes S.A. de C.V. incorpore para cumplir con estos requisitos deberá ser nueva y de uso exclusivo para el IMSS, no usada ni reconstruida.

De manera enunciativa más no limitativa, los requerimientos técnicos del IMSS en este sentido para con Operbes S.A. de C.V. son:

- Administrar la solución de seguridad propuesta para cumplir los requerimientos funcionales descritos. Adicionalmente, proporcionará en las instalaciones del IMSS (en la ciudad de México) un sistema de supervisión para todos los elementos de la solución, similar a la que se encuentre operando como parte de la solución de Operbes S.A. de C.V., para la comprobación de las funcionalidades requeridas por el

IMSS y que cuente con la capacidad de al menos 10 usuarios concurrentes.

- Poner en operación la solución localizada de seguridad basándose en las políticas operativas existentes en el ambiente de seguridad actual, mismas que serán compartidas por el Grupo Administrador del Contrato a Operbes S.A. de C.V. durante las mesas de trabajo. Se realizará un análisis de vulnerabilidades sobre la infraestructura global de red y sobre la propia solución de seguridad, a fin de que se identifiquen los aspectos de vulnerabilidad en la seguridad de la infraestructura del IMSS
- Proporcionar un esquema de replicación inmediata de las modificaciones en las políticas de los diferentes elementos y dispositivos que conformen la solución de seguridad específica para el Nodo CeNaTi D.F.
- Operbes S.A. de C.V. incluirá el hardware y/o software necesario para proporcionar al menos las siguientes funcionalidades tomando el diagrama como referencia:



- Solución en Alta Disponibilidad de Prevención de intrusos (IPS) que apoye a asegurar los servicios publicados por el IMSS y red interna Institucional y que soporte al menos 20,000 usuarios concurrentes
- Solución en Alta Disponibilidad de Firewall que soporte al menos 20,000 usuarios concurrentes
- Solución en Alta Disponibilidad de análisis de flujo (con capacidad de detección de anomalías en tráfico)
- Solución de Mitigación de Ataque de Negación de Servicios
- Solución en Alta Disponibilidad de Control de Acceso a Páginas Web (dimensionado por lo menos para 20,000 usuarios)

El canal de comunicación y capacidad de procesamiento de cada elemento en la solución de seguridad estará dimensionado con una política de al menos cuatro veces mayor al respectivo enlace a Internet, dependiendo del origen/destino de la información.

7.2.1.7. Funcionalidades Detalladas de Seguridad

A continuación, se describen con mayor detalle, las funcionalidades mínimas requeridas para cada uno de los servicios de seguridad asociados a los diferentes accesos (nodos) de Internet, de manera que obren como referencia para una adecuada selección de componentes habilitadores que permitan su entrega y cumplimiento bajo el esquema seleccionado de Servicios Administrados.

Todos los Componentes Habilitadores propuestos por Operbes S.A. de C.V. y requeridos para otorgar las soluciones de seguridad específicas que se enlistaron para cada uno de los Nodos de Internet previamente definidos, tendrán la capacidad de proveer las funcionalidades de seguridad solicitadas a continuación en cada servicio.

Operbes S.A. de C.V. incluirá en su propuesta un listado de los componentes habilitadores que integran cada uno de los servicios solicitados a continuación, indicando la marca, el modelo y las características de cada uno de ellos, demostrando de forma explícita de qué manera se atienden las funcionalidades mínimas solicitadas. Además, incluye diagramas con el diseño de alto nivel propuesto, en donde se identifique en forma clara y detallada la solución solicitada en cada uno de los servicios.

Con el fin de contar con un servicio homogéneo, todos los componentes habilitadores que sean propuestos por Operbes S.A. de C.V. para la integración de cada uno de los servicios específicos de seguridad serán del mismo fabricante. Lo anteriormente dicho no implica que todos los componentes habilitadores de todos los servicios de seguridad solicitados por el IMSS para los Nodos de Internet sean del mismo fabricante, sino que se mantiene esta condición para los componentes que integran las soluciones individuales (por ejemplo, la solución de firewall versus la de filtrado pueden ser de fabricantes distintos, pero todos los componentes habilitadores de cada una de ellas sí deberán de ser del mismo fabricante).

Operbes S.A. de C.V. observará, con independencia de los componentes habilitadores de seguridad elegidos, otorgar siempre al IMSS el cumplimiento de los Niveles de Servicio específicos, descritos en la sección "Requerimientos de Nivel de Servicio".

Adicionalmente, como requisito indispensable, Operbes S.A. de C.V. cuenta con el soporte, por parte de expertos del fabricante de cada una de las soluciones ofertadas, manteniendo así posibilidades de escalación directa con los mismos y sus respectivas áreas de desarrollo y soporte. Operbes S.A. de C.V. llevará a cabo, como parte del servicio asociado a cada una de las soluciones a detallar a continuación, de manera enunciativa más no limitativa, lo siguiente:

1. Provisión de los componentes habilitadores e instalación de los mismos en los nodos de acceso a Internet especificados en los Apéndices de esta contratación.
2. Interconexión de estos componentes habilitadores con los equipos de comunicaciones del Centro de Datos en cuestión.
   Para el "Nodo IMSS Digital", el Instituto solo brindará la coubicacion (energía eléctrica protegida y regulada, unidades de rack, puertos de Lan Switch y cableado estructurado).
   Por lo que Operbes S.A. de C.V., deberá indicar al Instituto lo correspondiente a la cantidad y tipo de puertos, contactos eléctricos con el amperaje y voltaje requerido, espacios en unidades de Rack y la infraestructura auxiliar que solicite.
3. Para los nodos de DF y Monterrey, el Instituto solo brindará espacio físico y energía regulada, por lo que Operbes S.A. de C.V. incluye en su proposición toda la infraestructura auxiliar que requiera
4. Configuración del equipamiento con base a las premisas de alto nivel expresadas en estos Anexos Técnicos.
5. Mantenimiento correctivo
6. Respaldo y reposición de equipo en caso de falla, respetando los Niveles de Servicio establecidos
7. Traslados a los sitios, considerando las horas de ingenieros para dar cumplimiento a los tiempos y condiciones explicados en este Anexo Técnico
8. Creación de los perfiles de la red del IMSS en las plataformas de administración correspondientes
9. Pruebas de turn-up de la red punta a punta, indispensables previo a la liberación y aceptación de cada una de las soluciones por parte del Grupo Administrador del Contrato en el IMSS
10. Altas, bajas y cambios.
11. Administración, gestión y operación.
12. Provisión de infraestructura auxiliar necesaria para la correcta operación de los servicios en los Centros de Datos mencionados, pudiendo ser ésta (de manera enunciativa mas no limitativa): racks, UPS, tierra física, cableado estructurado, entre otros.

7.2.1.8. **Solución o Capacidad de Mitigación de Ataque de Negación de Servicios (Clean Pipes)**
En la infraestructura de Operbes S.A. de C.V. se incluye un mecanismo para determinar en forma automática el comportamiento anómalo del servicio y tener la capacidad de alertar al IMSS para mitigar cualquier actividad

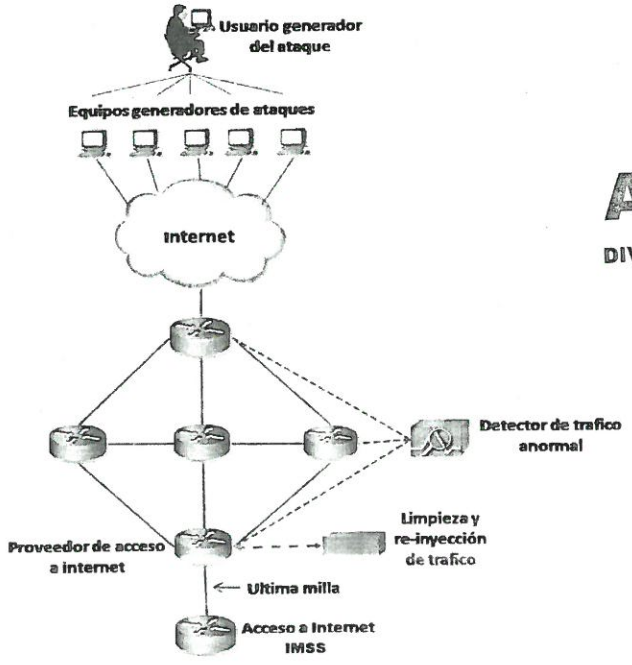
maliciosa que se presente, como ataques de negación de servicio o negación distribuida de servicio (DoS/DDoS, por sus siglas en inglés) generado por medio de la actividad de gusanos o de ataques de tipo botnets.

Como se mencionó anteriormente, esta solución o capacidad SÍ se encuentra integrada al precio unitario de los Servicios Administrados de Acceso a Internet de cada nodo, y no a los Servicios Administrados de Seguridad de cada nodo.

Por tanto, el servicio integrará un sistema de gestión de amenazas que realice una inspección profunda de paquetes, que permita a Operbes S.A. de C.V. reducir de manera rápida e inteligente las amenazas a la seguridad y contra cualquier situación desconocida que trate de agotar alguno de los recursos de los sistemas de comunicaciones, tales como el ancho de banda, saturación de búferes, saturación de discos duros o los recursos informáticos de la red.

A continuación, se mencionan algunas de las amenazas que, como mínimo, el sistema de mitigación de ataques de Operbes S.A. de C.V. elimina:

- Ping de la muerte
- Ataque por inundación SYN
- Fragmentación de paquetes y reensamblaje
- Broadcast de correo electrónico
- Saturadores de CPU
- Scripts generadores de tráfico
- Generadores de caracteres
- Ataques fuera de banda (WinNuke)
- Ataque Smurf (generador de gran cantidad de paquetes ICMP)



La funcionalidad de protección ofrecida tiene las siguientes características:

Monitoreo y Detección

- Ingeniería de tráfico inteligente: Visibilidad escalable y análisis del tráfico con tecnología de "Flujo de

Red"

- El análisis del tráfico con la tecnología de "Flujo de Red" se realiza en los enrutadores de Operbes S.A. de C.V., y de manera indispensable, en el equipo que provee el servicio de Internet a los enlaces del IMSS, en los enrutadores conectados a Internet y en los enrutadores conectados a Internet de sus demás clientes.
- Tanto la limpieza del tráfico como la re-inyección de éste, deberán realizarse lo más cercano posible al equipo CPE que entrega el servicio de Internet por parte de Operbes S.A. de C.V..
- Se garantiza el paso transaccional legítimo.
- Se mantiene una operación libre de problemas para los recursos críticos del negocio.
- Detección del tráfico basado en el lenguaje TCPDUMP (con información definida en las capas 3 y 4), será posible utilizar el Netflow para la revisión de TCP DUMP siempre y cuando cumpla con lo solicitado en el numeral de referencia y los niveles de servicios.
- El sistema tendrá la capacidad de advertir anticipadamente algún posible ataque, analizando tendencias de tráfico malicioso en tiempo real.
- Operbes S.A. de C.V. tendrá capacidad de monitoreo en tiempo real de los circuitos dedicados que entregan la conectividad a Internet para detectar el comportamiento anormal del tráfico que pueda estar dirigido a atacar las interfaces de los enrutadores implicados en el enlace.
- Operbes S.A. de C.V. tendrá la capacidad de monitoreo en tiempo real de la subred (pública) que conectan los enlaces, para que permita la detección de tráfico anormal que pueda significar un ataque dirigida a ella.
- Operbes S.A. de C.V. tendrá la capacidad de monitoreo en tiempo real de los activos informáticos conectados en la subred pública para detectar tráfico anormal que pueda significar un ataque dirigido a éstos.
- Detección de ataques basado en la línea de base contra los recursos definidos, con opciones configurables por recursos que permitan filtrar la sensibilidad de la anomalía y disparar una alarma, en paquetes por segundo y Mbps.
- Operbes S.A. de C.V. monitoreará las siguientes variables en tiempo real para garantizar los Niveles de Servicio:
  - Para el protocolo IP:
    - ICMP
    - Paquetes IP fragmentados
    - Paquetes IP NULL
    - Paquetes IP con direcciones privadas
  - Para el protocolo TCP:
    - Segmentos TCP NULL
    - Segmentos TCP RST
    - Segmentos SYN
    - Tráfico total
- La funcionalidad propuesta por Operbes S.A. de C.V. como mínimo detectan los siguientes tipos de ataques DoS/DDoS sobre las interfaces, subredes y activos informáticos protegidos del IMSS:
  - ACK Flood
  - SYN Flood
  - Hogging CPU
  - Chargen (Character generator)
  - FIN Flood
  - ToS Flood
  - DNS Malformed
  - HTTP Flood
  - ICMP Flood
  - UDP Flood
  - Non- UDP/TCP/ICMP Protocol Flood
  - PPS Flood Attack

- Zombie attack
- Land Attack

- La solución propuesta de Operbes S.A. de C.V. permite la personalización de los niveles de alarma o umbrales que sirvan para la detección de ataques, a una granularidad por objeto monitoreado.
- La solución propuesta por Operbes S.A. de C.V. monitoreará actividad sospechosa que pueda significar algún ataque de gusanos o "Worms" o virus.
- La solución propuesta por Operbes S.A. de C.V. monitoreará actividad "Dark IP"
- Detección de anomalías DDoS y amenazas de día cero antes de que impacten en los servicios.
- Por el detalle del monitoreo y detección, la solución propuesta por Operbes S.A. de C.V. estará basada en el uso del "Flujo de Red" en la red Operbes S.A. de C.V., más no en la red del IMSS, evitando la instalación de equipo para este propósito en las facilidades de dicha entidad.
- Detección de zombis (con selecciones de umbrales en Mbps y pps desde el portal Web del cliente) para clasificar una IP como zombis y con la opción de conocer una lista de zombis activos detectados.

Complementar la mitigación en la nube con la protección anti-DDoS en sitio para los portales web descritos en el anexo, incluir todos los elementos.

Mitigación:

- En el caso de que se tenga confirmación de un ataque detectado sobre el enlace, subred o activo del IMSS, Operbes S.A. de C.V. será capaz de ejecutar una mitigación apropiada para el tipo de ataque DoS/DDoS en progreso.
- Mitigación de DDoS y amenazas de día cero antes de que impacten en los servicios del IMSS
- Una vez que se ha detectado esta condición anómala, el tráfico deberá ser filtrado y descartado todo el tráfico dañino, dejando pasar solo el tráfico legítimo hacia las redes del IMSS para ser entregado a su destino final; durante todo este proceso los servicios publicados en Internet permanecerán siempre disponibles.
- Operbes S.A. de C.V. llevará a cabo la mitigación lo más alejado posible de la red del IMSS, ejecutándola en los puntos de interconexión de su red con otros proveedores de servicios ISP, para el caso de un ataque que provenga desde afuera de la red de Operbes S.A. de C.V., o bien se ejecutará en los enrutadores de acceso a Internet en el caso de un ataque originado desde la misma red de Operbes S.A. de C.V., evitando en todo momento hacerlo en los enlaces, subredes o activos del IMSS. Esto con el objetivo de mantener los recursos del IMSS disponibles para el tráfico legal.
- Operbes S.A. de C.V. comprobará al IMSS mediante documentación y diagramas topológicos de diseño, que la detección de flujos anómalos se realiza no solo en sus interconexiones principales de Internet, sino también a la infraestructura que provee el servicio de Internet al IMSS.
- El análisis del tráfico, la detección de anomalías y el proceso de mitigación de ataques de tipo DDoS se llevará a cabo en la infraestructura de Operbes S.A. de C.V., el objetivo es que el proceso de mitigación del tráfico de ataque se realice antes de que pueda llegar a las redes del IMSS.
- Durante la mitigación, Operbes S.A. de C.V. desviará el tráfico para limpiarlo, bloqueando o eliminando solo y únicamente el tráfico anómalo o ilegal, el tráfico normal o legal deberá de poder seguir usando los recursos del IMSS.
- Cuando Operbes S.A. de C.V. tenga confirmación de que el ataque ha terminado, el flujo de los datos seguirá su curso normal hacia el IMSS
- Para los ataques detectados, se ofrecerá la opción de generar recomendaciones de listas de acceso basadas en cada ataque.
- Se permitirá a Operbes S.A. de C.V. seleccionar la mitigación a aplicarse.
- La solución permitirá a Operbes S.A. de C.V. la inicialización de mitigaciones con:
  - Inyección de Blackhole de BGP
  - Filtros con listas de acceso (ACLs)
  - Dispositivos de mitigación que ofrecerán una mitigación inteligente, filtrar tráfico malicioso mientras se permite el tráfico válido para alcanzar el elemento que está siendo atacado

- Operbes S.A. de C.V. podrá implantar tecnología para procesar el máximo de ancho de banda de Internet de los enlaces solicitados.
- Permitirá ancho de banda adicional para ser adicionado hasta la petición del cliente
- La mitigación ofrecerá por lo menos las siguientes características:
  - Mitigación de específico SYN Flood
  - Mitigación del DNS (protocolo mal formado y basado en autenticación)
  - Mitigación con tasa límite por cliente de HTTP Get Flood y por objeto
  - Línea de base por recurso

Proceso de mitigación:

- Ante una alarma de tráfico anormal, Operbes S.A. de C.V. a través del centro de monitoreo contactará al personal designado por el IMSS para notificar del incidente y en su caso solicitar autorización para mitigar.
- Operbes S.A. de C.V. iniciará la mitigación de manera automática para el ataque DoS/DDoS "http flood" cuando así se haya pactado con el IMSS para este tipo de incidentes.
- Operbes S.A. de C.V. establecerá contacto con el IMSS mediante teléfono, teléfono móvil o correo electrónico.
- Operbes S.A. de C.V. garantizará que este será un proceso operativo en un marco de 7x24 horas los 365 días del año.
- Cuando el ataque haya sido mitigado, Operbes S.A. de C.V. notificará al Grupo Administrador del Contrato en el IMSS usando los medios descritos anteriormente.
- Si el IMSS llega a detectar algún comportamiento anormal, podrá contactar al centro de atención de Operbes S.A. de C.V. de servicio para verificar el estado de los recursos en términos de ataques de DoS/DDoS.
- Operbes S.A. de C.V. integrará en su proposición un esquema detallado de esta solución indicando los elementos que la integran, así como la descripción de los procesos de análisis de información, detección de anomalías y mitigación de ataques.
- Esta solución se requiere en la infraestructura de Operbes S.A. de C.V. (servicio ubicado en su nube)

Reportes:

- Operbes S.A. de C.V. facilitará al IMSS un portal Web para acceder a reportes vía Internet
- El portal Web proporcionará al IMSS toda la visibilidad de los ataques que están ocurriendo en su red.
- Se ejecutarán reportes en tiempo real y agendados que incluyan lo siguiente:
- Anomalías clasificadas por niveles de severidad (configurada por el IMSS)
- El Portal será personalizable, donde las plantillas puedan ser creadas para ver recursos específicos, reportes, ataques, así como, inicializar especificas mitigaciones y contador de medidas para reducir el impacto de esos ataques, todo desde la misma página Web
- Se proveerá acceso a al menos los últimos 3 meses de las alertas y las mitigaciones ocurridas
- Operbes S.A. de C.V. mostrará en pantalla estos reportes en hipertexto y gráficos usando navegadores Internet Explorer, Chrome y Firefox, hasta las versiones más recientes de éstos
- Los reportes podrán ser descargados por el IMSS en formato XML, PDF, Excel.xml y CSV
- El IMSS y Operbes S.A. de C.V. podrán enviar los reportes por correo electrónico desde el mismo portal hacia cuentas de correo de uso público, como cuentas internas del IMSS
- A través de la misma página Web deberá permitir la generación de plantillas de ataques conocidos
- Debe permitir a Operbes S.A. de C.V. generar reportes de las mitigaciones que fueron ejecutadas anteriormente, con detalles de tráfico que pasó y tráfico que se descartó para cada uno de los medidores, accesibles al IMSS
- Operbes S.A. de C.V. garantiza que los reportes como mínimo serán sobre:
  - Alertas "en proceso" y recientes, los cuales deben de mostrar:
    - Resumen de la alerta:
    - Identificación del evento

- Relevancia
- Impacto
- Hora de inicio y fin
- Dirección
- Tipo
- Recurso afectado

ANEXOS

DIVISIÓN DE CONTRATOS

- Caracterización del tráfico:
  - Fuentes y puertos
  - Destinos y puertos
  - TCP Flags
  - Protocolo
  - Gráficas del ancho de banda consumido contra tiempo, en bits- por- segundo y paquetes- por- segundo
- Elemento de red afectado
  - Relevancia
  - Valor esperado
  - Valor observado en bits por segundo
  - Valor observado en paquetes por segundo
  - Gráficas del ancho de banda consumido contra tiempo, en bits- por- segundo y paquetes- por- segundo
- Detalles del tráfico
  - Direcciones IP y máscara
  - Bytes
  - Paquetes
  - Bytes/paquete
  - Bits por segundo
  - Paquetes por segundo
  - % en bits por segundo
  - Rango de puertos
  - Protocolo
- Reporte sobre "Toptalkers" internos
  - Tabla que resuma el host y el peakrate
  - Gráfica de Toptalkers versus ancho de banda en bits por segundo y paquetes por segundo
- Reporte sobre "Toptalkers" externos
  - Tabla que resuma el host y el peakrate
  - Gráfica de Toptalkers versus ancho de banda en bits por segundo y paquetes por segundo
- Reporte sobre protocolos
  - Tabla que resuma el protocolo, dirección de In o Out, total y % de total, con valores actual, promedio y máximo
- Reporte sobre Tamaños de paquete:
  - Tabla que resuma el tamaño del paquete, In, Out y total, con valores Actual, promedio y máximo.
  - Gráfica de ancho de banda en bits por segundo y paquetes por segundo, dirección de entrada o salida versus el tiempo
- Reporte Alert Dashboard
  - Tabla y gráfica que resuma la identificación del evento, la importancia, el impacto, la duración, hora inicio y fin, tipo y recurso
- Reportes sobre gusanos (Worms) y Dark IP
  - Tabla que resuma el host y la tasa de transmisión

La Solución de Mitigación de Ataque de Negación de Servicios contará con un sistema de gerenciamiento (consola de administración) centralizado que realiza aprovisionamiento basado en políticas, configuración de dispositivos, gerenciamiento de actualizaciones, monitoreo y control de los dispositivos involucrados.

La Solución de Mitigación de Ataque de Negación de Servicios contemplará ser compatible con la mayoría de los correlacionadores de eventos comerciales disponibles en el mercado. Asimismo, se proveerán, integrados en el precio unitario de los servicios, los dispositivos (hardware, software e infraestructura auxiliar), que permitan que la solución de opere de acuerdo a los niveles de servicio solicitados.

7.2.1.9. **Solución de Prevención de Intrusos (IPS):**
Como se mencionó anteriormente, esta solución o capacidad se encuentra integrada al precio unitario de los Servicios Administrados de Seguridad de cada nodo.

Operbes S.A. de C.V. ofrece en esta solución, hardware de propósito específico que ofrece, como mínimo, las funcionalidades descritas a continuación:

Generales:

- Permite el paso del tráfico en el segmento de red sin afectar el funcionamiento de la red (Bypass)
- Tiene la capacidad de soportar la alta disponibilidad en modos activo-pasivo y activo-activo. Además, debe soportar balanceo de carga internamente en el appliance.
- Tiene la capacidad de soportar alta disponibilidad en modo de protección y simulación
- Soporta el ruteo asimétrico, además de soportar el monitoreo de redes MPLS. Para su cumplimiento se aceptan cartas siempre y cuando vengan firmadas por el representante legal del fabricante, debiendo acreditar su personalidad.
- Soporta el monitoreo de VLANs, incluyendo frames 802.1q y sensores virtuales internamente en el equipo.
- Realizará un monitoreo transparente para los usuarios, donde de forma automática bloquee ataques maliciosos, preservando la disponibilidad del ancho de banda de red.
    - La solución soporta la detección y prevención de intrusos a servidores y a la red
- La solución no requiere la modificación de los routers o switches funcionando como un puente en la red.
- Soporta el funcionamiento simulado; es decir, funcionamiento activo semejante al de prevención en línea, pero sin bloquear tráfico. El sistema sólo alerta qué eventos serían bloqueados.
- Permite la creación de reglas y filtros de acceso. Los criterios necesarios son, al menos, poder aplicar reglas por adaptador, VLAN, protocolo, origen y destino.
- Soporta funcionamiento simulado: funcionamiento activo semejante al de prevención en línea, pero sin bloquear tráfico. El sistema sólo alertará sobre los eventos que serían bloqueados.
- Soporta la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo de forma simultánea, cuando se refiere a IDS (pasivo) quiere decir que es un IPS que puede funcionar en modo de captura de paquetes sin realizar acción preventiva alguna.

Operbes S.A. de C.V. ofertará los IPS en base al ancho de banda máximo solicitado durante la vigencia del contrato.

Detección y de Bloqueo de Ataques:

- La solución operará en la capa 2 del modelo de OSI y el monitoreo que detecte debe ser de:
    - Accesos no autorizados a los distintos recursos que se encuentren en la red
    - Ataques o violaciones en el uso de los recursos de red del IMSS
    - Violaciones a las políticas definidas
    - Intentos de acceso o firmas de ataque (attack signatures)
    - DoS, spyware, códigos maliciosos, gusanos, backdoors, aplicaciones P2P
    - Análisis de Active X que pueda descargar código malicioso previniendo "dialing home", se refiere a que el IPS pueda realizar análisis del tráfico de Active X que ejecutan los navegadores

detectando así, cualquier código malicioso.

- Tiene la capacidad de identificar y bloquear tráfico de aplicaciones instant messenger y P2P, con soporte mínimo para las aplicaciones con las funcionalidades mencionadas abajo:
  - AOL Instant Messenger: AIM File Transfer, Login, Mensaje enviado, contraseña cambiada, Inicio de cifrado de datos
  - MSN Messenger: MS Messenger Login, Mensaje enviado a un cliente
  - Yahoo Messenger: Yahoo transferencia de Archivos, loging, Mensaje enviado a un cliente, Yahoo messengerMessenger Chat
  - Gnutella, Gnutella conexión de un cliente, descarga de Gnutella, detección del cliente limewire
  - Kazaa, Kazaa Cliente detectado, descargas vía cliente FastTrack
  - eDonkey: Edonkey cliente detectado
  - BitTorrent: en intento de conexión, solicitud de GET un cliente
  - SoulSeek, SoulSeek detección del cliente al servidor
  - DirectConnect: Direct Connect estableciendo una conexión cliente servidor
  - Monitoreo de inspección tipo stateful
  - Interface de monitoreo en modo stealth, sin stack de TCP/IP en la interfaz
  - Detección de ataques independiente del sistema operativo

Se acepta que la solución IPS pueda identificar y en dado caso bloquear el tráfico P2P, independientemente de la aplicación utilizada.

- Se consideran al menos las siguientes tecnologías de detección y bloqueo de ataques:
  - Identificar el protocolo a partir del puerto utilizado (Port Assigment)
  - Identificar los protocolos que utilizan puertos aleatorios (Port Following)
  - Permite la identificación del protocolo usado en la mayoría de las conexiones que se inspeccionen (Análisis de contenido)
  - Identificación de protocolos, aun cuando éstos estén encapsulados (Protocol Tunneling Recognition)
  - Análisis heurístico
  - Análisis de protocolo. Con decodificación de al menos 165 protocolos y formatos de datos de la capa 2 a la capa 7 del modelo OSI, permitiendo la detección de ataques desconocidos o variaciones de ataques conocidos sin utilizar firmas. Operbes S.A. de C.V. entregará listado de los protocolos soportados e incluir al menos los siguientes: SIP, Compound Files, Java script, HTML, MSRPC, http.
  - Detección de escaneo de puertos (Port Probes)
  - Permite la detección de ataques desconocidos o variaciones de ataques conocidos a partir de firmas basadas en vulnerabilidades
  - ReensambladoRFC Compliance Checking - verificación de compatibilidad con las RFC's
  - Formatos de Archivos - identifica al menos 30 formatos de archivos. Algunos de los solicitados son: BMP, CAB, EXE, GIF, HTML, JAVA, MDB, SWF, URL, ZIP, MIME. Se entiende que las tecnologías de detección a lo que hace referencia dicho punto, se refieren al análisis de potenciales vulnerabilidades y código malicioso en los formatos de archivo mencionados.
  - TCP Reassembly - reensamblado de paquetes fragmentados
  - ReensambladoFlow Reassembly - reensamblado de sesiones fragmentadas
  - Tiene la capacidad de analizar al menos los siguientes protocolos de VoIP: SIP, MGCP, Http Skype, H225 y H323
- Permite la detección de anomalías de tráfico a partir de análisis estadístico
- Permite firmas definidas por el usuario mediante el uso de regular expressions
- Presenta resistencia al menos a las siguientes técnicas de evasión:
  - IP fragmentation
  - TCP Stream Fragmentation
  - RPC Fragmentation

- URL Obfuscation
- Mutación Polimórfica y Alteración del protocolo

- Provee al menos los siguientes criterios de cuarentena:
  - Dirección del sistema víctima
  - Puerto del sistema víctima
  - Dirección del intruso
  - Puerto del intruso
  - Código ICMP
  - Tipo de ICMP
  - Duración de la cuarentena

Administración:

- Podrá administrarse de forma centralizada, a través de una sola consola del mismo fabricante, se considera, como parte de la oferta, una consola de administración.
- Soporta la integración de Syslog (número ilimitado de dispositivos)
- Soporta el ajuste dinámico de severidad en los ataques, como resultado de la correlación de eventos
- Soporta la correlación de datos de vulnerabilidades
- Soporta la comunicación de datos en forma cifrada
- Podrá generar reportes en formato texto y gráfico, con exportación a formatos HTML, PDF y CSV
- Capacidad de envío de eventos como mínimo por SNMP
- Soporta la administración remota vía Web con interfaz gráfica, para el uso en modo de consulta de dispositivos y eventos de seguridad
- Puede realizar de manera remota y automática su actualización y configuración de políticas
- Soporta la creación de múltiples roles, en el cual se permita o niegue el acceso a los diferentes dispositivos, o se den y revoquen privilegios para la administración, visualización de eventos y generación de reportes
- Tiene la capacidad de poder realizar automáticamente actualizaciones de software vía remota o Web para asegurar una protección en tiempo real. Las actualizaciones aplicadas no requieren de la reinicialización del componente habilitador
- Incluye una Base de datos de soporte (knowledge base) accesible a través de Internet que contiene una base de datos de referencia con cada una de las nuevas vulnerabilidades descubiertas, para ser analizadas y estudiadas como futura referencia

7.2.1.10. **Servicio de Firewall:**

Como se mencionó anteriormente, esta solución o capacidad se encuentra integrada al precio unitario de los Servicios Administrados de Seguridad de cada nodo.

Operbes S.A. de C.V. ofrece en esta solución, el hardware y/o software necesario que cuente con las siguientes características y que ofrezca las funcionalidades descritas a continuación:

Generales:

- Posibilidad en modos de operación transparente y gateway
- Soporte a enlaces redundantes para Alta Disponibilidad o balanceo de cargas, tanto para conexiones en texto claro como cifradas dentro de VPN de manera nativa en el firewall
- Cuenta con la capacidad de soporte en Alta Disponibilidad de al menos activo-pasivo y activo-activo, es decir, sin pérdida de conexiones en claro, cifradas, o clasificadas por el QoS, en caso de que un nodo falle
- Cuenta con soporte a Balanceo de cargas entre gateways de Firewall/VPN/QoS
- Soporta los protocolos SNMP RFC 1157, SNMPv2c o SNMPv3
- Cuenta al menos con una de las siguientes certificaciones:
  o ICSA
  o Common Criteria EAL3+ o superior

o FIPS 140 –Level 2 o superior
o TISEC E3

- Soporta al menos las siguientes tecnologías de red: Ethernet, Fast Ethernet, Gigabit Ethernet
- Soporta ruteo dinámico (por lo menos OSPF, BGP y RIP)
- Cuenta con la capacidad de hacer NAT estático (uno a uno); así como dinámico (muchos a uno), configurables de forma automática (solo especificando IP fuente e IP traducida)
- Cuenta con soporte a NAT para VoIP (tecnología de Voz sobre IP)
- Soporta la tecnología de QoS basada en colas inteligentes. Se proporciona funciones de QoS como: Encolamiento de prioridad, para tráfico que no puede tolerar latencia. Encolamiento jerárquico de prioridad (para crear una cola de tráfico prioritario dentro de otra cola)
- Soporta el monitoreo gráfico en tiempo real del tráfico de QoS que está circulando por el dispositivo directamente en el equipo Firewall o en el equipo CPE.
- Hace administración de Ancho de Banda por IP fuente, IP destino, dirección (hacia adentro o hacia fuera), URLs definidos por el usuario y horario
- Capacidad de hacer administración de ancho de banda por usuario o grupos de usuarios
- Soporte a límites (máximo ancho de banda a usar), garantías (mínimo reservado) y pesos relativos (prioridades) como acciones para el tráfico clasificado. Limitar o bloquear otras aplicaciones intensivas en su consumo de ancho de banda para otorgar más espacio en ancho de banda para aplicaciones críticas de negocio del Instituto, es la acción mínima para garantizar la prioritización del tráfico clasificado.
- Analiza las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs
- Especifica políticas tomando en cuenta puerto físico fuente y destino
- Define políticas de firewall que sean independientes del puerto de origen y puerto de destino.
- Las reglas del firewall toman en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando
- Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino
- Las reglas de firewall pueden tener limitantes y/o vigencia en base a tiempo
- Las reglas de firewall pueden tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)
- Soporta la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos
- Puede definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)
- Capacidad de hacer traslación de direcciones estático, uno a uno, NAT
- Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT
- Capacidad de bloquear equipos y ponerlos en cuarentena cuando estos no cumplen con políticas de seguridad o son identificados como generadores de tráfico malicioso
- Proporciona protección y soporte al menos a las siguientes tecnologías de Voz sobre IP: SIP, H.323, MGCP y SCCP (Skinny) para tráfico cifrado y calidad de servicio
- Puede hacer filtraje dentro de puertos TCP conocidos, aplicaciones potencialmente peligrosas como P2P aun y cuando se haga "tunneling" de estos simulando ser tráfico legítimo del puerto
- Soporte a aplicaciones Web y sus mecanismos de comunicación, tales como XML/SOAP.
- Soporta al menos los siguientes servicios: DCE RPC de Microsoft, NFS y SQL
- Capacidad de protección de tráfico de correo basándose en los tipos MIME en los archivos anexos (attachments), rechazar código ActiveX o Java, verificación de cumplimiento de los RFC relevantes; y que se tomen medidas para prevenir negación de servicio, tales como el máximo número de receptores, tamaño máximo de mensaje y máximo número de comandos erróneos

VPN seguras:

- Tiene integrada una solución de VPN, por si se planea adicionar soporte a VPN posteriormente

- Realiza configuración central de todos los dispositivos de VPN, sin que sea uno a uno.
- Soporta para esquemas VPN site-to-site en topologías "Full Meshed" (todos-contra-todos), Estrella (oficinas remotas hacia una oficina central), "Hub and Spoke" (tráfico entre oficinas remotas, pasando por inspección central), además de VPNs client-to-site (VPNs de Acceso Remoto)
- Capacidad de establecer VPNs entre nodos remotos con IP dinámica en topologías estrella y malla
- Soporte integrado para VPNs sin cliente mediante SSL, permitiendo flexibilidad en la comunicación VPN desde equipos a los que no pueda instalársele un cliente.
- Soporta para que se puedan establecer VPN usando clientes tipo L2TP
- Soporta VPNs con algoritmos de cifrado: AES, DES, 3DES.
- Soporta longitudes de llave para AES de 128, 192 y 256 bits
- Soporta al menos los grupos de Diffie-Hellman 1, 2, 5 y 14
- Soporta los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256
- Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site
- La VPN IPSec puede ser configurada en modo interface (interface-mode VPN). Es solvente la propuesta que habilite la funcionalidad "interface-mode VPN" referenciada bajo un nombre distinto.
- En modo interface, la VPN IPSec puede tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y ser capaz de estar presente como interface fuente o destino en políticas de firewall
- Tanto para IPSec como para L2TP soporta los clientes terminadores de túneles nativos de Windows y MacOS XSoporte a que los clientes de VPN puedan ser integrados con firewall personal (usando el mismo software) y verificador de configuración, con política administrada centralmente por la misma consola de la VPN. Los clientes de VPN que se propondrán podrán verificar la existencia de un firewall personal en la máquina cliente, mas no deben forzosamente tener la capacidad de la gestión de la solución de firewall personal.
- Tendrá capacidad de soportar VPNs cliente-a-sitio (client-to-site) basadas en SSL, que sean iniciadas en cualquier equipo que cuente con browser compatible y que sean terminadas en el gateway de VPNs
- Soporta las VPNs SSL siendo capaz la solución de verificar la legitimidad del cliente remoto efectuando un escaneo del equipo pudiendo detectar aplicaciones maliciosas como malware y spyware impidiendo el acceso del usuario en caso de que se detecten dichas aplicaciones
- Las cantidades correspondientes por tipo de tunel (IPSec, SSL) será soportados por la solución son IPSEC al menos 1000, SSL al menos 50.
- Para una mayor escalabilidad y facilidad administrativa, contención de fallos, a propuesta de Operbes S.A. de C.V., siempre y cuando cumpla con lo establecido en el numeral de referencia y los niveles de servicio podrá utilizar equipos separados de la solución de firewall para las funciones de VPN. Incluso, dada las diferencias de características entre un tunel sitio-a-sitio (IPSec) y un túnel cliente-a-sitio, es posible separar el tráfico de estos dos tipos de túneles, Operbes tomo en consideración que se aceptan propuestas en donde el equipo Firewall haga las funciones de VPN y las propuestas donde el equipo VPN sea distinto al equipo Firewall.

Administración:

- La solución de Firewall se administrará de forma centralizada a través de una sola consola de administración y monitoreo de políticas de firewall, VPN y QoS, en un solo equipo central con funcionalidades de monitoreo en tiempo real y reporteo
- La consola de administración tendrá la capacidad de definir administradores con diversos roles, con distintos permisos dentro de la consola para poder delegar funciones administrativas
- Soporta la autenticación fuerte (certificados) de manera nativa en la solución, para los administradores de la consola. Bajo el entendido de que una autenticación fuerte se logra bajo la integración con servidores de One-Time Passwords (o Tokens) que operan con el protocolo RADIUS, Operbes S.A. de C.V. tomó en consideración que se aceptan propuestas que logran la autenticación fuerte solicitada mediante la integración con servidores RADIUS, a propuesta de Operbes S.A. de C.V., siempre y cuando cumpla con lo establecido en el numeral de referencia y los niveles de servicio.

- Cuenta con la capacidad de dar seguimiento a los cambios realizados en la(s) política(s) de seguridad, de modo que sea posible revisar qué administrador hizo qué modificaciones, así como fecha, origen e impacto/alcance de la modificación
- Tiene la capacidad de generar bitácoras, que permitan obtener fácilmente un reporte completo del estado de la seguridad en la red
- Cuenta con una Interfase gráfica de usuario (GUI), para hacer administración de la solución, además de una Interfase basada en línea de comando
- Cuenta con una Interfase basada en Web para el acceso remoto considerando que la comunicación deberá de ser encriptada vía SSL al dispositivo firewall
- Tiene la capacidad de poder realizar una integración transparente y certificada con directorios tipo LDAP
- Tiene la capacidad de revisión de bitácoras en tiempo real
- Tiene la capacidad de poder generar versiones de la política de seguridad, y poder regresar a versiones anteriores de la misma
- Tiene la capacidad de monitoreo en tiempo real del tráfico circulando a través de los módulos administrados y monitoreo de sesiones, además de monitorear el estado de cada uno de los puntos de refuerzo (Firewalls, VPN's) que se encuentren en toda la red, en tiempo real
- Puede realizar mediciones de conexiones por segundo, conexiones concurrentes y paquetes por segundo que están pasando a través del firewall y desplegarlas al usuario administrador en tiempo real desde la interfaz de administración (no mediante línea de comando). Bajo el entendido de que los paquetes por segundo es un dato importante, pero un dato que puede resultar más valioso es la medición throughput (Kbps) que pasa por el firewall, se aceptan propuestas de desplegar el throughput utilizado gráficamente o la gráfica de paquetes por segundo.
- Tiene capacidad de generar reportes sobre el estado de los componentes, tráfico de red, y de las políticas de Firewalls, además de poder personalizar dichos reportes y de poder desplegar varios tipos de reportes en una sola ventana
- Tiene capacidad para presentar reportes del estado de Túneles de VPN en tiempo real y en reportes históricos
- Permitirá graficación en tiempo real de los "top N" servicios más utilizados y de los equipos que están consumiendo más ancho de banda
- Tiene capacidad de generar acciones y/o alertas en función de determinados eventos como cambios de políticas o valores críticos en contadores como uso de al menos CPU, Memoria y Disco
- Tiene capacidad de monitoreo y reacción sobre comportamiento de usuarios detectando actividades sospechosas, tales como intentos de acceso no autorizados permitiendo el bloqueo de las conexiones detectadas
- Tiene capacidad de realizar actualizaciones centralizadas del software, de forma remota
- Realiza configuración central de todos los dispositivos de VPN, sin que sea uno a uno Tendrá capacidad de hacer actualizaciones de software de firewalls sin importar que la versión sea menos reciente que la actual versión de la consola de administración
- Tiene capacidad de envío de eventos como mínimo por SNMP.

La solución de Firewall cuenta con un sistema de gerenciamiento (consola de administración) centralizado que realiza aprovisionamiento basado en políticas, configuración de dispositivos, gerenciamiento de actualizaciones, monitoreo y control de los dispositivos de seguridad.

La solución de Firewall será compatible con la mayoría de los correlacionadores de eventos comerciales disponibles en el mercado y opera de acuerdo con los Niveles de Servicio establecidos

7.2.1.11. **Servicio de Análisis de Flujo:**

Como se mencionó anteriormente, esta solución o capacidad se encuentra integrada al precio unitario de los Servicios Administrados de Seguridad de cada nodo.

Operbes S.A. de C.V. ofrece en esta solución los dispositivos necesarios que cuenten con las siguientes funcionalidades, mismas que permitan mostrar en tiempo real el flujo de tráfico de red del IMSS:

- Los cambios en el nivel de tráfico serán detectados en comparación con el tráfico observado previamente
- Detecta patrones de tráfico que sean diferentes a comportamientos predeterminados
- El servicio detecta escaneos lentos, rápidos, escaneos "stealth" y barridos de computadoras
- Puede definir una política y detectar violaciones contra la misma
- Puede detectar usuarios utilizando indebidamente recursos de red independientemente de dónde estos se hubieran logueado.
- El servicio permite la detección de comportamientos de worm
- El servicio cuenta con actualizaciones de las últimas amenazas en Internet, comparar esas amenazas con el tráfico existente en la red y alertar con base en esas amenazas
- El servicio soporta al menos los siguientes formatos de flows:
    - NetFlow v5
    - NetFlow v7
    - NetFlow v9
    - sFlow v2
    - sFlow v4
    - sFlow v5
    - Juniper cflow
- El servicio interpreta ruteo asimétrico
- El servicio posee un firewall propio para auto protección del mismo que rechace toda comunicación por default haciéndolo transparente a pings y host scans. Asimismo, siempre y cuando cumpla con lo establecido en el numeral de referencia y los niveles de servicio, se permite presentar propuestas que agregue un control de tráfico confiable dentro de la misma consola de administración con el fin de proveer un bloqueo de tráfico por rangos de IPs, lo cual asegure que se rechaza toda comunicación no conocida / validada por el Instituto y logrando incrementar el nivel de seguridad de la solución.
- El servicio posee un dispositivo central (analizador) que colecte flows, capturas de paquetes y los analice; así como dispositivos extras (colectores) que colecten flows, capturen paquetes y reporten al analizador.
- El servicio soporta un mínimo de 3 flows y 200 Mbps de captura de tráfico (modo sniffer)
- El sistema de detección de anomalías puede monitorear la tasa de tráfico de un determinado host/subnet y detectar cuando el tráfico exceda o sea inferior a niveles especificados. Estos niveles deben pueden ser ajustados basados en la hora del día y el día de la semana
- El producto puede ensamblar dos flows unidireccionales de distintos elementos de red y reensamblarlos en una sola conversación
- Las alertas de worms permite crear una lista de los hosts infectados y detalla el tráfico de worm en ese puerto de aplicación, comparado con el tráfico que no es del worm en el mismo puerto de aplicación durante el mismo período de tiempo
- El producto posee la habilidad de buscar las características de tráfico de un host, subnet, múltiples subnets o múltiples hosts y crear una política sobre ese tráfico. El sistema puede alertar cuando el tráfico difiere de la política
- El producto incluye ambas interfaces: consola local Gráfica y Línea de Comando
- Operbes S.A. de C.V. tomó en consideración que la consola Centralizada podrá ser la misma para productos de IPS de red, IPS de servidor, correlación de eventos y elementos de escaneo de vulnerabilidades o independiente si las soluciones no son del mismo fabricante. Lo anterior siempre y cuando se cumpla con lo solicitado en las especificaciones técnicas y niveles de servicio Estas funcionalidades se deberán proporcionar a través del SOC.
- El producto posee reportes que muestren los tops 5,10, 20, 50 y 250 talkers de la red junto con la cantidad de tráfico que cada host consumió.
- El producto posee reportes que muestren los top talkers que se comunican con un solo host o subnet en la red.

- Los reportes pueden ser exportados a pdf, xml y csv.

La Solución de Análisis de Tráfico cuenta con un sistema de gerenciamiento (consola de administración) centralizado que realiza análisis y reportes basado en políticas; gerenciamiento de actualizaciones.

Como se mencionó anteriormente, esta solución o capacidad se encuentra integrada al precio unitario de los Servicios Administrados. Operbes S.A. de C.V. ofrecer en esta solución, el hardware y/o software necesario que cuente con las características y que ofrezca las funcionalidades solicitadas.

7.2.1.12. **Servicio de Control de Acceso a Páginas Web:**

Como se mencionó anteriormente, esta solución o capacidad se encuentra integrada al precio unitario de los Servicios Administrados de Seguridad de cada nodo.

Operbes S.A. de C.V. incorporará en esta solución, el hardware y software o appliance de propósito específico que ofrezca las funcionalidades descritas a continuación:

- Posee más de 22 millones de URL's en la lista de sitios
- Las URL's estas clasificadas bajo más de 90 categorías y todas las categorías permiten bloquear o permiten el acceso, así como permiten el acceso con cuotas de tiempo, o permiten el acceso tras la aceptación de un término de responsabilidad
- Las URL's están clasificadas según su contenido diario, es decir, en el caso de que el contenido de una URL sea cambiado, el día siguiente ya está reclasificada bajo la categoría que refleje su nuevo contenido, para mantener la confiabilidad de la base de datos se requiere que sea actualizada por el mismo fabricante de la solución.
- Posee mínimo las siguientes categorías de URL's:
    - Banners y publicidad
    - Narcóticos
    - Sitios de almacenamiento personal de archivos y datos
    - Sitios de armas y municiones
    - Sitios de chateo por Internet
    - Sitios de compartido de archivos P2P
    - Sitios de compras y subastas
    - Sitios de contenido adulto o sexual
    - Sitios de contenido repulsivo
    - Sitios de descarga de MP3
    - Sitios de descarga de software gratis o pago
    - Sitios de hackers
    - Sitios de ilegales
    - Sitios de juegos o apuestas en línea
    - Sitios de mensajería instantánea
    - Sitios de phishing, spyware, adware, key loggers, inclusive aquellos sitios inocentes de otras categorías que hayan sido usados para hospedar phishing; luego de ser descontaminados, volverá a sus categorías originales
    - Sitios Web potencialmente maliciosos basadas en la "reputación", más allá de las técnicas de filtrado tradicionales.
    - Sitios que despliegan zombies, (BOT Networks) que utilizan las redes internas para generar ataques de Negación de Servicio (DoS por sus siglas en Ingles), robo de identidad, robo de información, etc.
- Identifica amenazas de seguridad, como spyware, spyware drive-by, bots y tráfico de redes bot, códigos maliciosos, phishing, pharming y keylogging; y bloquear el acceso en el gateway de Internet
    - Sitios de proxies públicos usados para evitar proxies corporativos (proxy avoidance)
    - Sitios de radio y televisión en línea
    - Sitios hacia los cuales los spyware, addware y keyloggers envían los datos recolectados de las

victimas
  - Sitios o páginas de correo electrónico vía Web
  - Sitios personales y bloggers
  - Sitios que contienen video o audio (streaming), aunque pertenezcan a otra categoría, tal como noticias, deportes, etc.
  - Sitios sobre alcohol y tabaco
  - Sitios sobre violencia y terrorismo
- Garantiza que nuevas páginas cuyo contenido represente riesgos a la seguridad sean agregadas automáticamente a la lista de URL's máximo cinco minutos después de haber sido descubiertas por el fabricante de la solución, durante el transcurso del día y de manera automatizada. Estas actualizaciones tendrán un registro del tipo de actualización que se llevó a cabo en función de las categorías, para mantener la confiabilidad de la base de datos se requiere que sea actualizada por el mismo fabricante de la solución.
- Permite la reclasificación manual de cualquier página Web según las necesidades, o bien permitir que ciertas páginas puedan ser accedidas en cualquier momento, aunque pertenezcan a categorías bloqueadas
- Permite el ingreso de URL's o bien de Expresiones Regulares (RegEx) para reclasificación manual
- Permite el bloqueo de páginas que pertenezcan a categorías permitidas, pero cuya URL posea ciertas palabras "clave"
- Permite el acceso a páginas de ciertas categorías, pero bloquear el intento de ciertos tipos de archivo (tales como video, audio, archivos comprimidos, ejecutables, documentos, etc.) desde dichas páginas
- Los tipos de archivos permite la personalización por tipo de extensión del archivo, así como la creación de nuevos tipos de archivos, aunque no sean comúnmente encontrados en la Internet
- Operbes S.A. de C.V. tomó en consideración que la consola de donde se realice la configuración/control/monitoreo podrá ser la misma que para los equipos IPS o independiente si las soluciones no son del mismo fabricante. Lo anterior siempre y cuando se cumpla con lo solicitado en las especificaciones técnicas y niveles de servicio.
- Reconoce transparentemente a los usuarios de las siguientes maneras:
  - Usuarios de Dominios NT
  - Usuarios de Active Directory
  - Usuarios de Novell eDirectory
  - Usuarios LDAP autenticados por RADIUS
- Pide autenticación manual a aquellos usuarios que intenten navegar sin estar debidamente autenticados en el servicio de directorio, sin pedir autenticación manual a los demás usuarios. La herramienta puede tomar las credenciales del usuario para validar su rol en directorio activo si la herramienta ya se encuentra asociada y recibe información e interactúa con dicho directorio
- Permite la definición de una política general que aplique a aquellos usuarios que no tengan una política específica asignada
- Permite diferentes tipos de bloqueo por horarios del día y días de la semana para cualquiera de las políticas definidas, el Instituto requiere bloqueo por horarios del día y días de la semana para cualquiera de las políticas definidas.
- Permite la definición de montos de cuotas de tiempo distintos para usuarios de grupos distintos, para usuarios específicos y para los usuarios generales
- Exhibirá una página HTML personalizable cada vez que un usuario intente acceder a una página bloqueada
- Pide confirmación al usuario cada vez que sea necesario usar su cuota de tiempo para navegar hacia cualquier página que pertenezca a una categoría que haya sido definida como permitida con el uso de las cuotas de tiempo a través de una página HTML personalizable.
- Permite a los usuarios acceder a sitios controlando el tipo de operaciones que pueden ejecutar para evitar riesgos relacionados a consumo de ancho de banda, productividad en los empleados o fuga de información.
- Habilitación de búsquedas seguras en motores de búsqueda, incluyendo multimedia en los buscadores

como "Ask", "Google", "Yahoo", "Bing", "Lycos", "YouTube"

- Permite control granular sobre redes sociales y sus aplicaciones como: "publicar mensajes", "enviar email", "email", "subir fotografías", "subir videos", "juegos", "mensajería instantánea". En sitios como: Vkontakte, Twitter, Sina, MySpace, Linkedin, Friendster, Facebook, Classmates, Bebo, Odnoklassniki, Google Plus, Orkut, RenRen, Mixi, entre otros, será suficiente demostrar que se cuenta con el control granular sobre redes sociales y/o Web2.0, y que los sitios mencionados son meramente informativos.
- Permite control de correo electrónico Web, Clips de Audio y video, Mensajería instantánea Web, y aplicaciones Web generales. Así mismo, los controles granulares por cada tipo de aplicación como "Enviar correo", "Subir archivo anexo", "Descargar audio", "Descargar video", "Subir video", "Play sobre video", entre otros.
- Permite la definición de políticas en las cuales ciertos usuarios puedan usar sistemas de Mensajería Instantánea libremente; otros usuarios no puedan usar sistemas de Mensajería Instantánea, y ciertos usuarios los puedan usar, pero al intentar enviar o recibir cualquier archivo adjunto, deberán ser bloqueados
- Permite la definición de políticas de uso de Protocolos por IP, rangos de IP's, usuarios y grupos de los siguientes servicios de directorio:
    - Dominios del Microsoft Windows NT (NTLM)
    - Dominios del Microsoft Active Directory
    - Directorios LDAP
    - Directorios Novell eDirectory
        - Deberá reconocer transparentemente a los usuarios dePing Sweep
        - Pruebas UDP (User Datagram Protocol)
        - Huella del dispositivo
        - Descubrimiento rápido
        - Descubrimiento por NetBIOS
        - Descubrimiento por TCP (Transfer Control Protocol)
        - Descubrimiento de Puertos UDP
        - Identificación de Sistema Operativo
        - Identificación de la Aplicación

En lo que se refiere a los directorios de Novell, será suficiente con demostrar la compatibilidad del directorio activo basado en Novell

- Cuenta con al menos las siguientes maneras, integradas al filtrado HTTP:
    - Usuarios de Dominios NT
    - Usuarios de Active Directory
    - Usuarios de Novell eDirectory
    - Usuarios LDAP autenticados por RADIUS
- El mecanismo de mantenimiento permite la programación de tareas automáticas para horarios predefinidos
- El mecanismo de mantenimiento será accesible desde la Web
- Posee interfaz de generación de reportes basados en templates predefinidos, los cuales permitirá el filtrado por usuarios, grupos de usuarios, categorías, clases de riesgos, acción tomada por el sistema, fechas y rangos de fechas
- La interfaz de generación de reportes permite a personal autorizado la generación de resúmenes, reportes detallados, gráficas y tablas sencillas
- La interfaz de generación de reportes permite exportarse los reportes generados para mínimo los siguientes formatos:
    - Microsoft Word (Opcional)
    - Acrobat PDF
    - HTML
    - CSV
- La interfaz de generación de reportes permite la programación de múltiples tareas de generación de

reportes predeterminados, en horarios y días de las semanas predefinidos, y deberá:
  - Enviar los reportes generados por correo electrónico hacia los recipientes deseados
  - Publicar los reportes generados en una página de la Intranet
  - Copiar los reportes generados hacia una carpeta local o en la red
- Posee interfaz de acceso directo a los registros de log a través de la Web, utilizando el concepto de drill-down
- La interfaz de acceso directo a los registros de log permite que cada criterio de datos se pueda expandir según otro criterio, generando informes de múltiples niveles
- La interfaz de acceso directo a los registros de log permite que cualquier pantalla de visualización se pueda exportar para archivos de Microsoft Excel o bien para el formado Adobe Acrobat PDF
- La interfaz de acceso directo a los registros de log permite la personalización de los reportes generados
- Se puede generar reportes de Riesgos de Seguridad presentes, como que usuarios/IP han sido atacados con Spyware, Phising, Addware, Keyloggers, etc.
- Se generarán reportes en función de cuánto ancho de banda consumen estas clases de riesgos (bytes Enviados/Recibidos/Total)
- Estos mismos reportes de riesgos, tendrán información que permitan hacer análisis forense para poder identificar y erradicar dichos riesgos
- Se podrá configurar que se manden dichos reportes por correo de manera periódica
- Se podrá configurar que se envíen alertas en tiempo real, a correo electrónico o en pantalla, sobre estos riesgos, a detalle, con información sobre Usuario/IP, Categoría accedida, Sitio/URL, IP del Sitio, la disposición (si fue bloqueada o permitida de acuerdo a las políticas), hora y fecha
- La interfaz de acceso directo a los registros de log permite la generación automática de reportes y su distribución por correo electrónico

La solución de Control de Acceso a páginas web cuenta con un sistema de gerenciamiento (consola de administración) centralizado que realiza aprovisionamiento basado en políticas, configuración de dispositivos, gerenciamiento de actualizaciones, monitoreo y control de los dispositivos.

Operbes S.A. de C.V. podrá ofertar una solución que integre ambas funcionalidades Firewall, IPS y control Control de Acceso Web, siempre y cuando cumpla con los niveles de servicio requeridos.

7.2.1.13. Portal de Información Preventiva ante Vulnerabilidades Detectadas en Internet

Esta solución o capacidad se encuentra integrada al precio unitario de los Servicios Administrados de Seguridad de cada nodo.

Operbes S.A. de C.V. cuenta para la administración y prevención de incidentes en Internet con un Portal que muestre el comportamiento del tráfico actual en Internet con respecto al histórico, así como alertas o avisos de seguridad. Este portal será accesible tanto para sus propios operadores del servicio como para al menos 5 usuarios concurrentes definidos por el IMSS, a su vez el acceso será desde la red interna e internet.

El Portal de Seguridad contiene lo siguiente:

- Vista en una gráfica de las últimas 24 horas de la utilización de la red de Internet (en bytes o conexiones o una combinación de ambos) de Operbes S.A. de C.V., por tipo de tráfico o aplicación, así como una proyección de la utilización para las próximas 6 horas y un comparativo contra la utilización histórica. Esta vista será utilizada para identificar y detectar de forma temprana cualquier actividad inusual del tráfico en Internet. El tipo de tráfico o aplicación a monitorear para su utilización son:
  - Peticiones / respuestas de protocolo web (HTTP /HTTPS)
  - Aplicaciones punto a punto (FTP, P2P)
  - Infraestructura (p. ej. ICMP, DNS, protocolos de ruteo)
  - Mensajería (SMTP, POP, IMAP, IRC etc.)
- Utilización actual (por hora) de la red de Internet para los puertos más utilizados del protocolo TCP, UDP, ICMP e IP con un comparativo de la utilización actual contra el valor histórico para la misma hora

del último mes.

- La capacidad de presentar la utilización (en flujos, bytes o paquetes) de forma gráfica con respecto al total del tráfico para cualquier puerto de TCP o UDP para diferentes rangos de tiempo (hora, día, o semana en curso).
- Generación por parte del usuario de reportes de utilización por puerto de protocolo TCP, UDP, ICMP e IP para un periodo de tiempo definido (último mes).
- Los reportes de utilización de puertos generados por el usuario se desplegarán las alertas de seguridad o avisos generados para ese puerto en particular.
- La utilización de puertos por las aplicaciones por protocolo de transporte como TCP y UDP (puertos del 0-65535) o tipos para ICMP (tipos del 0 al 255), medida en flujos con respecto al total de flujos del protocolo (TCP, UDP o ICMP) considera para cada puerto lo siguiente:
    - Utilización actual de flujos del puerto en porcentaje con respecto al total del protocolo
    - El promedio de utilización histórico de las últimas semanas (3 a 5 semanas) del puerto con respecto al total para el protocolo.
    - Factor de cambio de la utilización actual con respecto al histórico.
- El portal presenta alertas de eventos de seguridad en la red de Internet basadas en monitoreo del tráfico, del análisis y la correlación con vulnerabilidades conocidas. Las alertas estarán clasificadas por tipo o severidad con al menos 3 niveles o tipos:
    - Alerta comprobada (para un incremento de tráfico asociado a una vulnerabilidad o ataque, puede causar un daño potencial y requiere una acción).
    - Advertencia (para un incremento de tráfico inusual sin asociación a un ataque).
    - Advertencia Limitada (para detección de ataque en algún punto focalizado de la red de Internet, pero que se traduce en un mal comportamiento generalizado en la red).
- Las alertas de seguridad contarán con recomendaciones asociadas de actividades de contención y/o erradicación. Por ejemplo, bloqueo de tráfico de ciertos protocolos, o aplicación de parches para sistemas.
- Las alertas tendrán asociada una vista del tráfico en el momento de su generación para el puerto específico afectado y mantenerla como referencia histórica.
- El portal mostrará avisos de seguridad. Los avisos de seguridad son advertencias de amenazas nuevas o preexistentes sobre servicios (DNS/HTTP/HTTPS) o sobre vulnerabilidades reportadas en productos o plataformas específicas por parte de proveedores. Los avisos de seguridad cubrirán tecnologías comunes para su rápida identificación como:
    - Microsoft Windows/DOS
    - Solaris/ Sun OS
    - Peoplesoft
    - IBM AIX
    - Cisco IOS
    - Bases de datos
    - APPLE
    - Oracle
    - Unix
    - Email
    - Seguridad/Firewall
    - Linux
    - Correo
    - Equipo Genérico de Red
- La información resumida de los avisos de seguridad contendrá al menos: Fecha de publicación, descripción o resumen, ID dentro del portal, proveedor.
- La información detallada de los avisos de seguridad contendrá la siguiente información
    - Número de control
    - Asunto
    - Clasificación

  - Proveedor
  - Producto
  - Puertos
  - Protocolo
  - Fecha
  - ID de Alerta del producto
  - Número de Parche
  - Sistemas vulnerables
  - Resumen de la vulnerabilidad
- Operbes S.A. de C.V. tomó en consideración que se considera deseable que el portal de seguridad pueda ser accesible en forma segura (acceso duro) desde un dispositivo externo tipo smartphone o tablet, siempre y cuando el dispositivo sea accesible de acuerdo a las especificaciones establecidas en la presente propuesta.
- Operbes S.A. de C.V. tomó en consideración que *es importante destacar que no se aceptan soluciones de software libre, distribución gratuita, código abierto o sin soporte del desarrollador (fabricante).*
- Operbes S.A. de C.V. tomó en consideración que *el Instituto requiere gráficas de lo descrito en cada una de las funcionalidades mínimas solicitadas, siempre y cuando no impacte en los servicios solicitados.*

El portal con la Información de Seguridad en Internet contará con las siguientes funcionalidades:

- Disponibilidad del Portal de Seguridad de 7x24x365.
- Mostrará la información en inglés o español. El idioma será configurable en el portal o en el navegador.
- Autenticación del usuario mediante usuario y contraseña para el acceso a la información. Se proporcionará autenticación para el acceso a la información, exclusivamente.
- Ligas (hipervínculos) hacia otros sitios de seguridad relevantes. Los sitios mínimos a los que apuntará podrán ser sitios de los fabricantes de su propuesta técnica, Centros de Respuesta a Incidentes, security focus, osvdb, secunia, cert.org, zone-h, cve.mitre.org. Los anteriores sitios serán considerados como enunciativo más no limitativo.
- Explicación de alertas de forma detallada con apoyos multimedia cuando sea posible
- Noticias recientes de la industria sobre seguridad de información o recomendaciones de buenas prácticas de seguridad por parte de expertos en el tema. Operbes S.A. de C.V. tomó en consideración que el posible proveedor adjudicado alimentará la información, y será visible en el portal y enviadas por correo.
- Desplegará el nivel de alerta de la red de Internet alineado con la escala de colores de Homeland Security Advisory System de los Estados Unidos: Verde = Bajo, Azul =En Guardia, Amarillo = Elevado, Naranja =Alto, Rojo = Severo, Gris = Normal (sólo valido para tráfico)
- Una vista rápida de resumen alertas, avisos o utilización de puertos y ligas hacia reportes detallados
- La vista rápida de alertas tendrá una descripción de las alertas más severas, asunto, fecha y resumen y desplegarlas en orden cronológico. El usuario tendrá la capacidad de ordenarlas o realizar búsquedas por Fecha, ID o Descripción
- La vista rápida de avisos contendrá al menos asunto, fecha, vulnerabilidad y resumen, ordenados de forma cronológica. El usuario tendrá la capacidad de ordenar o realizar búsqueda de avisos de seguridad por fecha, por proveedor, o por tipo o por descripción
- La vista rápida de utilización de puertos contendrá al menos puertos de interés y su utilización actual (como porcentaje del total), utilización promedio histórica y factor de cambio entre la utilización actual y el promedio histórica.
- Los reportes detallados de utilización para un puerto específico tendrán asociados las alertas y avisos para ese puerto.
- El usuario podrá configurar notificaciones por correo electrónico para cuentas específicas y establecer criterios para recibir tanto las alertas como avisos. El aviso por correo electrónico tendrá información suficiente para su valoración y una liga a la descripción detallada en el portal. La definición de alertas debe considerar:

- Configuración por parte del usuario del nivel de alerta a configurar (alerta comprobada, advertencia o advertencia limitada)
- Configuración por parte del usuario de alertas sólo de los puertos/tipos de interés para TCP, UDP, ICMP o IP.
- Las alertas puertos de interés pueden configurarse de la siguiente manera:

Para TCP y UDP:
+ Para todos los puertos (0-65535)
+ Para puertos bien conocidos (well known ports) (0—1023)
+ Para puertos registrados (0-49151)
+ Para puertos dinámicos (49152-65535)
+ Para puertos bajos (0-2047)
+ Subrangos

Para ICMP:
+ Todos los tipos (0 a 255)
+ Tipos originales (0 a 16)
+ Tipos Extendidos (17 al 40)
+ No usados o experimentales (41 a 255)

- Configuración por parte del usuario de avisos sólo para ciertas plataformas o tecnologías, de tal forma que se reciban sólo sobre aquellas que son de su interés

7.2.1.14. Monitoreo a la Disponibilidad a servicios WEB

Operbes S.A. de C.V., a través del SOC, monitoreará a través de un medio de comunicación diferente, independiente y externo a la red del Instituto, las páginas, sitios, portales o aplicaciones Web del Instituto publicados y visibles desde Internet; con la finalidad de verificar que están funcionando o estén alcanzables (activos y en condiciones normales de operación). En caso de que algún sitio o URL se inhabilite, no responda o trabaje inadecuadamente, se alertará inmediatamente al personal que el Grupo Administrador del Contrato designe. Estas páginas o sistemas web tienen direcciones públicas iguales o similares al dominio "*.imss.gob.mx".

El monitoreo de disponibilidad a servicios Web del Instituto ejecutará de manera permanente durante toda la duración del contrato para hasta 20 sitios o URL´s que el Instituto indique a Operbes S.A. de C.V. Se proporcionará el servicio de monitoreo a través de una herramienta automatizada con la cual se verifique, en intervalos regulares, la disponibilidad del servicio HTTP/HTTPS para cada uno de los sitios definidos por el Instituto.

La herramienta de monitoreo estará en el SOC de Operbes S.A. de C.V. y éste brindará el acceso a la herramienta vía HTTPS, mediante cuentas con rol de solo lectura, tanto de forma interna a la red del Instituto como de forma externa (a través de Internet).

El intervalo de poleo será inicialmente de 300 segundos para cada sitio.
Operbes S.A. de C.V. tomó en consideración que el Instituto requiere que se notifique al personal que éste designe, cualquier pérdida de disponibilidad y recuperación con base en los puntos que se adjuntan a continuación. En caso de que el personal del IMSS no pueda ser localizado vía telefónica, Operbes S.A. de C.V. enviará en paralelo un mensaje de voz, un mensaje SMS al celular del contacto y un correo electrónico.

- Si el servicio no responde en el intervalo de poleo, se enviará otros tres intentos dentro de los siguientes 120 segundos.
- En caso de que no se haya restablecido la disponibilidad, Operbes S.A. de C.V. tomó en consideración que el Instituto requiere que se compruebe la pérdida del servicio de forma manual a

través de un enlace independiente al utilizado por la herramienta de monitoreo.
- En caso de comprobar la no disponibilidad del servicio, se notificará al personal designado por el IMSS.
- En el momento de que se detecte la recuperación y estabilización del servicio, por al menos 30 minutos, se notificará al personal designado por el Instituto.

Operbes S.A. de C.V. tomó en consideración que el Instituto requiere que los registros de la herramienta se almacén por al menos un mes en el repositorio de información del servicio y serán entregados, en formato electrónico, cuando el MSS los requiera. Asimismo, Operbes S.A. de C.V. generará de forma mensual un reporte con la siguiente información: 1) página monitoreada (dominio y dirección IP), 2) descripción de los problemas de indisponibilidad presentados en el período y 3) tiempo promedio de indisponibilidad.

Operbes S.A. de C.V. tomó en consideración que es importante destacar que no se aceptan soluciones de software libre, distribución gratuita, código abierto o sin soporte del desarrollador (fabricante).

7.2.1.15. Servicios Operativos

A continuación, el IMSS describe los distintos Servicios Operativos que serán indispensables para complementar adecuadamente los servicios administrados de Red Privada Virtual, Internet, por lo que son considerados integrales y homologados a los mencionados.

Todas las labores de servicios y operación descritas a lo largo del presente propuesta técnica, tales como: soporte técnico, optimización, mantenimiento preventivo y reactivo, puesta a punto, ajustes finos, mejoras, actualizaciones de hardware, software, firmware y firmas de seguridad, altas, cambios, bajas de configuraciones, análisis de fallas, análisis de desempeño, auditorías y demás servicios requeridos para la correcta operación de los Servicios, así como el cabal cumplimiento de los Niveles de Servicio Requeridos para cada uno de los Servicios estipulados en este documento de Propuesta Técnica y todas sus Secciones, serán consideradas como parte de los precios asociados a la provisión de sus respectivos Servicios Administrados (RPV e Internet). Operbes S.A. de C.V. tomó en consideración que el IMSS no incurrirá en ningún costo adicional por los Servicios de Operación descritos en esta propuesta Técnica, y en ninguna circunstancia ejercerá una erogación adicional asociada a los Servicios de Operación aquí descritos, ni mediante unidades de servicio desagregadas, soporte extendido, ni cualquier otro mecanismo de pago alterno y/o adicional.

Servicios de Monitoreo y Gestión

Operbes S.A. de C.V. tendrá la infraestructura y herramientas de monitoreo necesarias que permitan conocer el estado que guardan todos los componentes, infraestructura, equipos, enlaces y servicios que integran los servicios descritos en esta propuesta Técnica, independientemente de la configuración de equipos y funcionalidades que tengan cada uno de los nodos del IMSS, así como la capacidad de personalización de la información tanto en su presentación visual, como en los reportes que serán generados. Las herramientas mencionadas son parte de un servicio integral que se puede componer de más elementos conforme a la estrategia que oferte Operbes S.A. de C.V.

Operbes S.A. de C.V. ofrece la gestión del servicio de forma pro-activa, es decir, anticiparse a los problemas e incidentes que se puedan presentar durante la vigencia del contrato, vía el cumplimiento de los Niveles de Servicio establecidos; además dicho servicio debe estar diseñado para proveer el conocimiento del desempeño de los componentes de datos, video y voz en la RPV y en su seguridad.

El servicio se proporcionará de forma remota desde las instalaciones de Operbes S.A. de C.V., considerando redundancia a nivel de enlaces, además de contará con todos los recursos necesarios para la prestación del servicio los cuales aseguren el funcionamiento de la infraestructura habilitadora, parte del alcance de la presente contratación, en un esquema 7x24x365 y durante la vigencia del contrato. De igual manera, considera el personal de apoyo en sitio que se requiera, para cumplir con los niveles de servicio establecidos y para proporcionar la continuidad de la operación que requiere el IMSS.

Operbes S.A. de C.V. será el responsable de realizar en su totalidad la gestión del servicio, en todos los sitios; considerando al menos lo siguiente:

- Líder de Gestión del Servicio
- Mesa de Servicio
- Administración de problemas
- Administración de la configuración
- Administración de cambios
- Administración de los niveles de servicio
- Administración de las plataformas
- Monitoreo de las plataformas
- Mantenimiento de las plataformas
- Actualización de las plataformas

ANEXOS
DIVISIÓN DE CONTRATOS

Administración y Monitoreo

Operbes S.A. de C.V. se obliga a efectuar la administración y monitoreo de toda la infraestructura (Redes WAN, Internet y Seguridad), incluyendo gestión proactiva del aseguramiento del servicio, conociendo de manera preventiva los diferentes indicadores de niveles de servicio de la red en datos en todos los sitios a nivel nacional. Esta gestión se realizará de manera centralizada libre de costos adicionales al IMSS, con accesos seguros, como VPN, IPsec, SSH o HTTPS.

Se entiende que este monitoreo es proactivo y que todo el seguimiento será con los procesos automáticos, definidos por Operbes S.A. de C.V. y el Instituto en las mesas de trabajo, de tal forma que se cubran las funcionalidades y niveles de servicio solicitados.

El monitoreo proporcionará lo siguiente:

- Acceso vía web a los reportes generados por el sistema de monitoreo a través de cualquier PC bajo control del IMSS y se deberán considerar 5 (cinco) accesos simultáneos.
- Monitoreo en Tiempo Real de los componentes de acuerdo a los tiempos de muestreo acordados entre Operbes S.A. de C.V. y el Grupo Administrador del Contrato para la obtención de datos de la infraestructura, equipamiento, ruteadores, enlaces, servicios agregados como lo son los relacionados con la seguridad (firewall, IPS, etc.), y el demás objeto de la presente contratación
- Extracción e interpretación de datos relacionados con el estado y el desempeño de los dispositivos que componen a la RPV y servicios agregados como lo son los relacionados con la seguridad (firewall, IPS, etc.) y el demás objeto de la presente contratación

Se entenderá como consola de monitoreo el acceso remoto vía http a las herramientas de monitoreo y gestión del NOC para el personal asignado por el IMSS.

Líder de Gestión del Servicio:

Para la gestión del servicio, Operbes S.A. de C.V. designará un Líder, y en caso de que lo considere convenientes supervisores, los cuales serán notificados inmediatamente al Grupo Administrador del Contrato en caso de sustitución de personal.

Funciones mínimas del Líder:

- Coordinará la ejecución del Sistema de Gestión del Servicio. (Operación Diaria).
- Consolidación y entrega de los reportes mensuales.
- Convocatoria y conducción de las reuniones de seguimiento mensuales y extraordinarias en la materia.

Funciones mínimas del Supervisor:

- Coordinará al personal en sitio para que se elaboren los trabajos encomendados por el Líder de Gestión del Servicio.

- Llevar una bitácora de trabajos y/o incidencias.
- Elaborar reportes de avance mensuales donde se muestre el estado que guarda el servicio prestado.
- Asistir a las juntas de coordinación que sean programadas por el personal del IMSS.

Herramientas de Monitoreo

Para la operación del monitoreo de los niveles de Servicio, el proveedor debe proporcionar la infraestructura que considere necesaria para asegurar la correcta medición de los niveles de servicio solicitados en el proyecto descrito en este anexo técnico.

Vale la pena reiterar que es responsabilidad de Operbes S.A. de C.V. asegurará la correcta operación, dimensionamiento, soporte, gestión de dicha infraestructura para cumplir con los requerimientos y niveles de servicio establecidos en este proyecto.

De manera enunciativa, más no limitativa, algunas variables a monitorear en el servicio son:

- Disponibilidad
- Latencia
- Pérdida de paquetes
- Anchos de banda mínimos y máximos
- Porcentajes de utilización por enlace
- El crecimiento estará alineado con el crecimiento eventual del servicio hacia los máximos del contrato

Operbes S.A. de C.V. operará el Portal Web de monitoreo de servicios requeridos que soporte diferentes usuarios con diferentes niveles de privilegios para que además de poder generar reportes de las KPI del Centro de Datos, estas puedan ser visualizadas a voluntad. La herramienta entregará información en forma de reportes, variables, alertas y portales de modo que sea acorde a las mejores prácticas de ITIL. Las herramientas tanto de monitoreo y gestión, como de mesa de ayuda se podrán integrar y ofertar soluciones de distintos fabricantes que permita proporcionar la funcionalidad solicitada.

Como se mencionó anteriormente, las herramientas de monitoreo de niveles de servicio son del total responsabilidad de Operbes S.A. de C.V., desde su selección (siempre y cuando cumpla con al menos lo que se solicita en esta sección) hasta su puesta a punto, y será el encargado de darles el soporte adecuado para su correcto funcionamiento.

Entre las capacidades analíticas que se requieren para la herramienta de Gestión y Monitoreo de niveles de servicio para cada tipo de tecnología están al menos las siguientes:

Para los equipos: CPE

- Pruebas mínimas que se realizará:
  - Pruebas de conectividad
  - Prueba de integridad de datos: Que se demuestre que los datos enviados de un nodo origen llegan sin alteración a un nodo destino.
  - Prueba de saturación de enlaces: Detectar que los enlaces están siendo saturados a su capacidad permitida por cierto tipo de tráfico identificado.
  - Pruebas de tiempo de respuesta
  - Prueba de loops: Demostrar que las redes de comunicación no estén conectadas físicamente de tal forma que generen problema de bucle que deterioren los tiempos de respuesta o que generen caídas.
- Utilidades mínimas que incluirá
  - Ping
  - Traceroute
  - Tabla ARP
  - Tabla de enrutamiento

  - SNMP
- Métricas de desempeño mínimas que incluirá el reporte obtenido de la herramienta
  - Utilización del ancho de banda
  - Throughput
  - Disponibilidad
  - Latencia
  - Paquetes perdidos
  - CPU de los Componentes Habilitadores del servicio tercerizado
  - Memoria de los Componentes Habilitadores del servicio tercerizado

Para los equipos de seguridad:

- Pruebas mínimas que podrá realizar:
  - Pruebas de conectividad (ICMP)
  - Prueba de integridad de datos (ICMP)
  - Prueba de saturación de enlaces (Paquetes Perdidos)
  - Pruebas de tiempo de respuesta (Tiempos de ida y Tiempos de regreso)
  - Prueba de flujos TCP
  - Prueba de resolución de nombres (DNS)
  - Prueba de emulación de transacciones HTTP y HTTPS
- Utilidades mínimas que incluirá
  - Ping
  - Traceroute
  - Escaneo de Puertos
  - SNMP
- Métricas de desempeño mínimas que incluirá el reporte obtenido de la herramienta
  - Utilización del ancho de banda
  - Throughput
  - Conexiones por segundo
  - Conexiones concurrentes
  - Cantidad de traducciones NAT/PAT
  - Disponibilidad
  - Tiempo de respuesta
  - Paquetes perdidos
  - CPU
  - Memoria

Se alineará con la disciplina de Help Desk de ITIL, entregando una cuenta de perfil de Monitoreo IMSS al personal de Mesa de Servicio para que éste pueda observar la misma información que fue causante de una alerta, además de dar el seguimiento hasta el cierre de ésta. Capacidades suplementarias a las disciplinas de Service Level Management de ITIL, Availability Management de ITIL y Capacity Management de ITIL.

Los reportes deben poder ser solicitados por medio del portal de gestión del servicio por los usuarios facultados, en cualquier instante del contrato, y pueden ser accesados a través de este, o pueden ser programados para su envió vía correo electrónico en el instante, o por periodos de tiempo previamente programados (diario, semana, mensual).

La herramienta permitirá que se colecten métricas tipo NetFlows, sFlow y IP SLA de las infraestructuras de enrutamiento y conmutación de modo que se puedan a analizar los inventarios de Flujo de Información que la infraestructura pueda enviar a un colector centralizado en el Centro de Datos.

La herramienta de monitoreo de niveles de servicio será capaz de recibir el total de los flujos generados por el total de la infraestructura del servicio, dicha capacidad será calculada por Operbes S.A. de C.V. como parte de su propuesta.

La herramienta de monitoreo permitirá la administración y controles de acceso de usuario, tales como:

- Manejo de perfiles de usuario.
- Dispositivos y secciones de la aplicación a los que puede acceder el usuario.
- Privilegios para la generación y consulta de reportes.
- Acceso a vistas de estado y desempeño de la red en tiempo real.

Operbes S.A. de C.V. mantendrá a punto la herramienta de monitoreo de niveles de servicio, proporcionando las mediciones continuas a la infraestructura y servicios a su cargo.

Existirá al menos las siguientes vistas que aseguraran cuales son las tecnologías que impactan cada uno de los grupos de elementos que componen el servicio objeto de esta contratación para cumplir con las acciones proactivas que garanticen la continuidad de la entrega del servicio:

- Vista donde se muestre el conjunto de variables tales como métricas de medición y disponibilidad de los enlaces, módulos de servicios, capacidades de infraestructura, variables que impactan un servicio, de modo que el impacto en una de ellas impacte el estado de la vista y de la posibilidad de drill–down
- Vista de mapa de los recursos y su relación para detectar por medio del drill-down las variables impactadas.
- Alarmas a nivel infraestructura para detectar el impacto que este tiene en los servicios.
- Alarmas a nivel de servicio para alertamiento a alto nivel de impacto a grupos de recursos.
- Alarmas de tipo seguridad, donde se muestre el tipo de ataque, el objetivo del ataque y la mitigación de éste.

Para garantizar que los eventos que se presenten sean manejados de la forma más eficaz, se entregará mensajes de alertas de la siguiente naturaleza:

- Vía Correo Electrónico
- Vía Traps SNMP para eventuales sistemas de gestión
- Capacidad de configurar y ejecutar Scripts de notificación
- Mensajes Texto o SMS

Operbes S.A. de C.V. configurará al menos una comunidad SNMP con derechos de lectura, independiente a la comunidad que él utilice para el monitoreo de los diferentes equipos de comunicaciones y seguridad controlados por él y que formen parte del servicio descrito en la presente propuesta técnica.

Esta comunidad tendrá como objetivo monitorear todos estos equipos desde un sitio diferente al NOC, con uno o más servidores del IMSS (o un tercero definido por éste). En estos servidores se recibirá la notificación automática de incidentes y envío de traps SNMP, según parámetros establecidos por el IMSS, que permitan tener visibilidad sobre variables importantes de desempeño del servicio. En caso de que el IMSS lo requiera, Operbes S.A. de C.V. proveerá y configurará al menos una comunidad SNMP, sin menoscabo de agregar adicionales que no estén incluidas en este apartado. Las métricas que se requieren, ya sea por SNMP o MIBs, son las siguientes:

- Net Flow (SNMP, MIBs y/o solicitud por contrato) (Previa validación a través de una Mesa de Ingeniería IMSS-proveedor)
- IP Acc (SNMP, MIBs y/o solicitud por contrato) (Previa validación a través de una Mesa de Ingeniería IMSS-proveedor)
- Logs
- Configuraciones
- Consumo de ancho de banda por enlace

- Niveles de Servicio de disponibilidad y desempeño establecidos en el contrato

Los registros generados por la herramienta o herramientas de monitoreo serán los que se utilizarán para validar los niveles de servicio proporcionados por Operbes S.A. de C.V., de acuerdo con los requerimientos del IMSS, y bajo los niveles de servicio definidos en la sección Niveles de Servicio de este anexo técnico.

- En caso de controversia, la información recibida a través del protocolo SNMP y MIBs en los centros de monitoreo del IMSS, podrá ser utilizada como referencia para determinar si existen diferencias respecto a lo reportado por el NOC de Operbes S.A. de C.V., y en su caso, ser reconocidas como elementos de juicio para establecer un punto de acuerdo. Esta opción solo será prerrogativa del IMSS y nunca de Operbes S.A. de C.V.
- Con el objeto de contar con la información para controlar y monitorear los servicios proporcionados, Operbes S.A. de C.V. proporcionará los reportes correspondientes al desempeño del servicio, información que debe de ser entregada dentro de los primeros 10 días hábiles del mes siguiente. Dependiendo de la importancia del reporte, de común acuerdo con el IMSS, se establecerán las fechas de los reportes identificados como críticos
- Operbes S.A. de C.V. realizará todas las configuraciones necesarias, para dejar habilitado el acceso a los equipos para poder recolectar los datos que le permitirán generar los reportes correspondientes.
- El Cuerpo de Gobierno del IMSS validará y permitirá las configuraciones de acceso para la recolección de datos y para la presentación de reportes de acuerdo con las políticas de seguridad validadas por el personal facultado al interior del IMSS.

Centro de Operación de Seguridad (SOC)

Operbes S.A. de C.V. ofrecerá el monitoreo permanente de los elementos y servicios de seguridad solicitados durante la vigencia del contrato, con el fin de verificar el estado de cada uno de los elementos que lo soportan y tomar las acciones necesarias en caso de presentarse un evento que ponga en riesgo la operación del servicio. Para ello, el Posible Operbes S.A. de C.V. incluye en su Propuesta Técnica contar con un Centro de Operaciones de Seguridad (Security Operation Center, SOC, por sus siglas en inglés). El objetivo de este centro es el de la administración, supervisión, gestión y monitoreo de los elementos, servicios, soluciones y configuraciones de seguridad, mismas que realizará análisis proactivo y reactivo con el fin de proteger las aplicaciones e información interna de la Institución.

Operbes S.A. de C.V. oferta la integración de un programa de gestión de eventos conforme a los procesos y mejores prácticas de la industria de un SOC, a fin de proporcionar las funcionalidades y niveles de servicios solicitados.

La administración de la seguridad se comandará desde este Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés). Será monitoreado y gestionado en su operación por Operbes S.A. de C.V., en un régimen de 7x24x365, durante la totalidad de duración del contrato, y contará con la cantidad de ingenieros necesarios para cumplir los acuerdos de nivel de servicio y horarios solicitados.

El SOC estará suscrito a los principales sitios y listas de correo de Internet que notifican sobre nuevas vulnerabilidades. Cuando se detecte una nueva vulnerabilidad, el SOC realizará inmediatamente un análisis para conocer si afectará las operaciones del IMSS en lo que a la infraestructura objeto del contrato atañe; y si es viable, iniciará los procedimientos aplicables, así como emitirá los boletines para difusión al interior del IMSS en coordinación con el Grupo Administrador del Contrato.

El SOC contará al menos con dos procesos certificados en ISO/IEC 27001:2005 y contará con al menos dos personas adscritas al SOC certificadas en ITIL V3 Nivel Intermedio OSA y RCV., las cuales brinden los servicios directos al Instituto.

Los alcances y funciones que tendrá el SOC durante la totalidad de duración del contrato serán, de manera enunciativa más no limitativa:

- Operará en un régimen de 7x24x365, durante la totalidad de duración del contrato, y deberá contar con la cantidad de ingenieros necesarios para cumplir los acuerdos de nivel de servicio y horarios solicitados.
- Dará atención hasta su resolución de los incidentes de seguridad presentados.
- Monitorea permanente las actividades realizadas en la red notificando al personal que designe el IMSS en máximo 30 minutos todas aquellas actividades sospechosas que puedan comprometer la seguridad.
- Monitorea el estado de operación de los componentes de la infraestructura tecnológica de seguridad, así como recolectar las alertas que generen, normalizar y correlacionar la información que de ellas se deriven y emitir los reportes que serán enviados a los responsables de seguridad del IMSS, de tal suerte que puedan manejar y responder a potenciales incidentes de seguridad o incidentes en curso a fin de tomar las medidas necesarias para contenerlos.
- Administra la infraestructura de seguridad para mantener configuraciones óptimas a fin de asegurar la confidencialidad, integridad y disponibilidad de la información.
- Brinda el soporte para cualquier incidencia registrada por las herramientas y/o que le sea reportada.
- Actualización de memorias técnicas y documentos de control relacionados con elementos, soluciones y servicios de seguridad.
- Coordinación con otros recursos para atender casos de incidentes de seguridad de la Información.
- Reporta actividades sospechosas que puedan provocar un incidente de seguridad.
- Apoya en el monitoreo y trazabilidad de paquetes para apoyar en la determinación de puntos de indisponibilidad de servicios.
- Comunica al personal que designe el IMSS cualquier incidente de seguridad y/o actividad sospechosa con base en lo establecido en el apartado "Prioridades de Seguridad2 descrito en este documento.
- Realiza con base a la autorización emitida por el personal del IMSS las actividades de contención para minimizar los impactos ocasionados por la presencia de una actividad sospechosa o un ataque.
- Establece *Acuerdos* del Nivel de Operación (*OLA, por sus siglas en inglés*) con los terceros que el Instituto y los responsables de seguridad le indiquen.
- Resolver todas las fallas relacionadas con los dispositivos, soluciones y servicios de seguridad contratados, en coordinación con el personal de soporte en sitio y remoto solicitados en la sección correspondiente del presente documento "Soporte Técnico en Sitio y Remoto".
- Resolver todas las fallas relacionadas con los dispositivos, soluciones y servicios de seguridad contratado, basado en el modelo de gestión de fallas mencionado en la sección Atención a Fallas".
- Monitoreo de la salud de todos los dispositivos de seguridad habilitados para proporcionar los servicios y soluciones de seguridad considerando al menos: estado de la memoria, CPU, estatus de interfases y diferentes variables de los equipos
- Creación de reportes proactivos para los casos en que al detectarse o dispararse alguna alarma, se requiera especial atención, por ejemplo, violación de umbrales definidos de desempeño, caídas de interfases
- Notificación al personal que designe el IMSS en máximo 30 minutos, incluyendo el primer diagnóstico. El comunicado al cliente incluirá el evento detectado, así como las acciones a seguir y el estado del servicio (Severidad 1, Severidad 2, Severidad 3).
- Monitoreo en tiempo real de todos los dispositivos, soluciones y servicios de seguridad contratados.
- Capacidad para eventualmente interconectar el sistema de monitoreo del SOC, con un sistema designado por el IMSS, con el fin de acceder a información relativa a sus servicios con derechos de lectura.
- Capacidad para permitir al personal que designe el IMSS, para generar reportes explotando todas las variables y funcionalidades de la herramienta de monitoreo, con la opción de parametrizar dichos reportes y consultarlos vía Web.
- Notificación de las fallas de los servicios contratados al personal designado por el IMSS, por medio del proceso más apropiado (email, ticket de fallas, etc.)
- Soporte técnico en sitio o remoto para atender cualquier falla, incidente de seguridad o indisponibilidad

de algún servicio del Instituto; debiendo ser permanente durante toda la duración del contrato cualquier día natural y en cualquier horario.

- Notificación inmediata al personal que designe el IMSS, al momento en que se detecte una falla en los dispositivos, soluciones y servicios de seguridad contratados, debiendo entregar un reporte detallado con la solución en un periodo no mayor a 12 horas, cuando éste sea solicitado por escrito por el IMSS. Para los casos donde el incidente sea motivo para ejercer una penalización o deductiva, el reporte Post-Mortem tendrá que ser generado en automático. Para los casos en los que Operbes S.A. de C.V. haya incurrido en penalización o deductiva, el reporte se entregará en automático, sin necesidad de que el Cuerpo de Gobierno del IMSS lo solicite.
- Base de datos que almacene íntegramente el historial de información de los dispositivos, soluciones y servicios de seguridad contratados monitoreado en forma diaria, con periodos de registro según se acuerden en las mesas de trabajo entre Operbes S.A. de C.V. y el Cuerpo de Gobierno del IMSS, y que permita conservarla para ser consultada en cualquier momento al menos durante los 60 días naturales posteriores a su generación, sin realizar ningún tipo de sumarización o compactación de los registros durante este periodo de consulta. Esta base de datos almacenará dichos registros históricos en forma mensual, compactados, hasta la conclusión del contrato, y podrán ser solicitados por la Convocante en cualquier momento durante la vigencia del mismo. Los elementos a almacenar, así como los mecanismos para su acceso, serán acordados conjuntamente entre el Cuerpo de Gobierno del IMSS y Operbes S.A. de C.V. en un plazo no mayor a 30 días posteriores a la fecha de notificación de fallo de la contratación.
- Medición de Capacidades: El SOC llevará a cabo la contabilización de la utilización de los recursos de la infraestructura para proporcionar los servicios y soluciones de seguridad. Los sistemas de monitoreo recolectarán la información diariamente, para ser almacenada en una base de datos que estará disponible en cualquier momento para que el personal autorizado del IMSS pueda revisar y generar los reportes, a través de aplicaciones proporcionadas o desarrolladas por el SOC.
- Generación de Estadísticas: En este punto el SOC contará con aplicaciones que permitan generar, verificar y almacenar las estadísticas del desempeño, capacidad y utilización de cada uno de los elementos instalados para proporcionar los servicios y soluciones de seguridad, debiendo contar con un historial de los rubros descritos anteriormente; lo cual tomará en consideración para la elaboración de la planeación de capacidades (Capacity Planning). Este reporte será entregado de manera trimestral, y tendrá, al menos, un análisis detallado del comportamiento de los servicios proporcionados, y las sugerencias de mejora basadas en este análisis.
- Estar suscrito a los principales sitios y listas de correo de Internet que notifican sobre nuevas vulnerabilidades. Cuando se detecte una nueva vulnerabilidad, el SOC realizará inmediatamente un análisis para conocer si afectará las operaciones del IMSS en lo que a la infraestructura objeto del contrato atañe; y si es viable, iniciar los procedimientos aplicables, así como emitir los boletines para difusión al interior del IMSS en coordinación con el Grupo Administrador del Contrato.
- Tener su propia gobernabilidad y por ende ser totalmente independiente del Centro de Operación de Red (NOC, por sus siglas en inglés)
- Contar con procedimientos detallados para la administración de incidentes, manejo de alarmas y análisis de información y correlación de eventos, por lo que adjuntará copia simple de los mismos en su propuesta técnica. Operbes S.A. de C.V. en caso de resultar ser el proveedor, los procedimientos serán revisados en conjunto con personal del IMSS, o quien éste designe, para hacer las adecuaciones particulares, en caso de aplicar.
- Llevar un estricto procedimiento de Control de Cambios que considere tener documentado toda adición, modificación, eliminación de las configuraciones, reglas y/o políticas de los elementos, servicios o soluciones de seguridad; esto con la finalidad de mantener una base y/o memoria técnica actualizada al día de las configuraciones que se tiene en los dispositivos.
- Generar y proporcional al personal que designe el IMSS siempre que sea requerido los archivos (con contraseña) que contenga los respaldos sobre las configuraciones, reglas y/o políticas, diagramas, especificaciones de todos los elementos, servicios o soluciones de seguridad

El Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) cumplirá con lo siguiente:

Requerimientos Mínimos del SOC:

Con objeto de contar con una adecuada Administración de la Seguridad, Operbes S.A. de C.V. se compromete, en la presente propuesta técnica, a cumplir durante la totalidad de duración del contrato con:

- Operbes S.A. de C.V. cuenta con personal con experiencia comprobable en seguridad de información de 2 años como mínimo y con certificaciones en seguridad reconocidas.
- Operbes S.A. de C.V. empleará metodologías reconocidas internacionalmente, basadas en mejores prácticas como ISSAF, CoBIT, ISO/IEC 27001:2005 e ITIL en la prestación de los distintos servicios de seguridad de información que se requieran para el alcance de esta propuesta.
- Las áreas que brindarán el servicio de SOC al IMSS, estará certificadas en ISO/IEC 27001:2005 y en ITIL Management and Capability Level por lo menos.
- Operbes S.A. de C.V. cuenta con un proceso o procedimiento de administración de riesgos que le permita identificar y cuantificar riesgos y seleccionar los controles de seguridad correspondientes para garantizar los Niveles de Servicio acordados. se identificará y describirá brevemente dentro de su propuesta técnica el proceso de administración de riesgos (tales como OCTAVE o MAGERIT, por mencionar algunos) de seguridad de información utilizado en la prestación de sus servicios de seguridad de información.
- Operbes S.A. de C.V. tendrá documentado e implementado un proceso de administración de incidentes de seguridad de información, así como la conformación de sus equipos de respuesta y administración de incidentes. Describirá brevemente, como parte de su Propuesta Técnica, los mecanismos que utilizará para determinar la causa raíz de los incidentes que podrían afectar la seguridad de la información de los servicios proporcionados, así como sus respectivos canales de comunicación y contacto con entidades mayores para la solución de los mismos.
- Operbes S.A. de C.V. contará con la infraestructura exclusiva para el IMSS, necesaria para la administración, correlación, monitoreo y gestión de los dispositivos de seguridad incluidos en el contrato, siendo éstos de manera enunciativa más no limitativa, los Firewalls, IPSs, etc. Este servicio está incluido y dimensionado en cumplimiento a los requerimientos del presente contrato.
- Operbes S.A. de C.V. cuenta con un programa de auditorías, a intervalos planeados, internas, así como de terceras partes, para validar el cumplimiento que se tiene dentro de la empresa de políticas, proceso y procedimientos documentados como práctica regular asociadas con los servicios brindados, incluyendo el cumplimiento con regulaciones, normas y/o estándares internacionales.
- Operbes S.A. de C.V. cuenta con las medidas de protección física necesarias para garantizar que sólo personal autorizado tendrá acceso a los recursos de cómputo, comunicaciones e información reservada.
- Operbes S.A. de C.V. tiene y documenta el proceso utilizado para llevar a cabo la administración de vulnerabilidades, el perfil del personal involucrado, la(s) tecnología(s) utilizada(s) y el alcance del servicio (recomendaciones para el cierre de vulnerabilidades o cierre efectivo de vulnerabilidades). Todo ello con total apego a las disposiciones establecidas en el Manual MAAGTIC-SI.
- Operbes S.A. de C.V. cuenta y documenta los controles de seguridad que minimicen el riesgo que representan eventos de software malicioso, como virus, gusanos, troyanos, etc, así como el desarrollo de servicios y productos generados bajo un esquema de seguridad en su ciclo de vida.
- Operbes S.A. de C.V. cuenta procedimientos documentados e implementados de Control de Acceso, Registro de Usuarios y Administración de privilegios. Cuenta con listados de controles de acceso, administración de permisos y privilegios para el resguardo de la información. La administración de control de acceso está ligada al ciclo de vida de los empleados de Operbes S.A. de C.V.
- El personal adscrito al posible proveedor deberá tener firmados acuerdos de confidencialidad que cubran tanto los intereses del proveedor como los de sus clientes. Estos acuerdos de confidencialidad deberán ser revisados regularmente – al menos anualmente, a través de un proceso de revisión definido y documentado a petición del IMSS.

Operbes S.A. de C.V. tomó en consideración que la infraestructura ofertada por Operbes S.A. de C.V. para la partida 1 y 2 será independiente por cada partida. Operbes S.A. de C.V. tomó en consideración que en caso de que un proveedor resulte ganador en ambas partidas, podrán compartir exclusivamente el servicio de NOC y SOC correspondiente.

Repositorio de información

Operbes S.A. de C.V. incluye en su propuesta técnica un mecanismo de almacenamiento de información <Repositorio> no se requiere compatibilidad con otro repositorio que al menos contenga, a lo largo de la vigencia del contrato, la siguiente información:

- Infraestructura, es decir, el conjunto de componentes habilitadores detallando marca, serie, versión del sistema operativo o software instalado operando, modelo y principales características (RPV, acceso a Internet, así como herramientas de supervisión, monitoreo y seguridad, NOC y SOC) que formen parte de la solución deberán incluirse en el repositorio.
- Direcciones IP
- Mantenimientos
- Control de Cambios
- Monitoreo (Administración, Continuidad del Negocio)
- Respaldos
- Memoria Técnica detallando los servicios por inmueble, así como diagramas y características de los componentes habilitadores de la solución incluyendo las configuraciones.
- Incidencias
- Facturación
- Ciclo de vida
- Análisis de tendencias
- Plan de mejora de servicios
- Niveles de Servicio
- Tabla de escalación por servicio
- Detalle de la conformación general de la red e infraestructura de telecomunicaciones, así como qué porción es proporcionada por qué empresa del consorcio cuando se trate de participación conjunta.

Además, incluye los entregables de única vez y en caso de que sean susceptibles de ser actualizados, incorporará las versiones modificadas durante la vigencia del contrato. También contendrá el histórico de los entregables periódicos.

El respaldo se refiere a una copia de las configuraciones (versión de sistema operativo, configuración lógica, configuración física) actualizada de todos los CPEs de enrutamiento, seguridad, servicios agregados y equipos activos del servicio. El ciclo de vida se refiere a la fase del proyecto en la que se encuentra cada CPE, equipo activo o terminal (sustitución, operación, etc.).

Respecto a la facturación, solo será requerida aquella información técnica que permite observar la cantidad de servicios utilizados, su costo y aquellos reportes relacionados con el cumplimiento del nivel de servicio.

El repositorio de información permitirá acceder a la información mediante consultas a través del protocolo http al menos a 10 usuarios concurrentes que el IMSS designará.

El acceso a dicho repositorio será a través de autenticación proporcionada con login y password al personal designado por el IMSS, permitirá la configuración de roles identificados por usuarios, con el objetivo de mostrar la información de los ID's designados y creación de directorios clasificados por nodo, permitiendo el despliegue individual y privado de la información. La autenticación estaría asociada a otros mecanismos de acceso como LDAP/Directorio Activos, siempre y cuando cumpla con las funcionalidades y niveles de servicio solicitados

Los roles mencionados podrán ser de 3 tipos:

- "Lector", solamente puede ver los documentos publicados
- "Autor", puede ver los documentos publicados y no publicados, añadir documentos, crear o borrar sus propias carpetas; editar, borrar y publicar cualquier documento en el sitio
- "Aprobador", puede ver las carpetas y documentos a los cuales tiene acceso, y puede revisar, aprobar o rechazar documentos

Será responsabilidad del IMSS la administración del sistema de repositorio, aclarando que por administración se entiende altas, bajas y cambios de usuarios, manejo de privilegios, entre otros; y no el mantenimiento y operación de la infraestructura que forme parte de esta solución, mismo que es responsabilidad de Operbes S.A. de C.V.

La plataforma propuesta Operbes S.A. de C.V. tener las siguientes funcionalidades:

- Control de versiones. La herramienta dará seguimiento de los documentos e impedirá que alguien pueda sobrescribirlos y guardará una versión de cada documento en el que se hayan introducido cambios.
- Perfiles de documentos. La herramienta será capaz de agregar información a los documentos para plantear búsquedas de palabras clave, fechas de modificación o características, por ejemplo.
- Publicación de documentos. Los documentos publicados son accesibles para los usuarios del portal en vistas privadas o públicas. Puede especificarse cuándo y cómo se publicarán.
- Suscripciones. Cuando se encuentra información útil en el portal, es posible suscribirse a dicha información para conocer las últimas modificaciones y estar al día de los posibles cambios a que ésta se someta.
- Respaldos periódicos, programables y customizables.

Operbes S.A. de C.V. ofrece una solución en un solo repositorio, asegurando también que la explotación y acceso a la información será desde una sola herramienta y con capacidad de espacio de almacenamiento de 500 Gbytes como mínimo.

Esta consulta permitirá la exportación o descarga de la información contenida en el repositorio en los formatos nativos de cada una de ellas, conforme a los privilegios establecidos para cada tipo de usuario.

Operbes S.A. de C.V. asegurará que los equipos que operen en el servicio cumplan con un nivel de seguridad que mantenga la información acorde con los estándares y requerimientos que el área de Seguridad Informática del IMSS disponga. La infraestructura para proveer esta funcionalidad estará en las instalaciones de Operbes S.A. de C.V. y siempre y cuando se cumplan las funcionalidades y niveles de servicio solicitados.

El Repositorio de Información, incluyendo la plataforma y la información que en éste reside, pasarán a ser administrados por el IMSS o por quien éste designe, al final del contrato.

8. Condiciones de Continuidad.

Operbes S.A. de C.V. tomó en consideración que derivado de que el servicio objeto del presente contrato se prestará como continuidad al contrato DC17S0083 y su convenio modificatorio no.1 por un periodo adicional de siete meses, contados a partir del día siguiente a la notificación de adjudicación y hasta el 31 de diciembre de 2020, con el mismo proveedor que actualmente presta los servicios desde de enero de 2018 bajo el contrato DC17S0083 y su convenio modificatorio no.1, de forma enunciativa más no limitativa no serán aplicables aun cuando así lo mencione el presente contrato y su Anexo los siguientes conceptos:

- Las entregas únicas y primigenias previas al inicio de la prestación de los servicios

- El Periodo de habilitación, configuración, transición, pruebas, así como puesta a punto de los servicios objeto del presente Anexo y sus respectivos apéndices
- La entrega de manuales
- La sustitución de equipo de voz, datos o vídeo,
- Los equipos de seguridad perimetral, firewalls,
- La entrega de enlaces de telecomunicaciones ya existentes,
- El manual de la solución propuesta,
- Las topologías, certificaciones de seguridad, políticas, procedimientos y certificados en manejo de seguridad de la información,
- La matriz de escalación del servicio, incluyendo la entrega-recepción de la administración,
- Toda aquella documentación e infraestructura operativa, ya que Operbes S.A. de C.V. podrá usar toda su base instalada y operativa existente a la fecha.

De la misma manera, Operbes S.A. de C.V. tomó en consideración que por ser un contrato de continuidad de servicios, seguirán teniendo validez los documentos de comprobación administrativa y de descripción del servicio del contrato DC17S0083 y su convenio modificatorio no.1, asimismo quedan sin efecto los niveles de servicio, los periodos estipulados de gracia en la aplicación de penas convencionales y deductivas por concepto de transición de los servicios, ya que se trata de un contrato de continuidad. Los alcances y servicios, así como los niveles de servicio, penas convencionales y deductivas por tratarse de un contrato de continuidad serán las mismas que están estipuladas en el contrato actual DC17S0083 y su convenio modificatorio no.1.

Operbes S.A. de C.V. tomó en consideración que las condiciones aquí estipuladas prevalecerán en todo momento respecto a lo estipulado en el Anexo Técnico, Apéndices y Términos y Condiciones del presente procedimiento de contratación por lo que en caso de que existiera discrepancia de manera enunciativa más no limitativa en cuanto a los alcances, servicios, entregables y/o niveles de servicio, deductivas, penalizaciones entre otros, lo señalado en el presente numeral será prevalente sobre el presente procedimiento de contratación.

9. Perfil del posible proveedor.

ANEXOS
DIVISIÓN DE CONTRATOS

PARTIDA 1

Operbes S.A. de C.V. tomó en consideración que los siguiente entregables no aplica, ya que son para la partida 1, en la cual Operbes S.A. de C.V. no está participando.

A. El posible proveedor deberá incluir en su proposición documento en hoja membretada de la empresa en donde indique el personal asignado a los perfiles solicitados por el Instituto, así como la documentación del mismo.

- Líder del proyecto: El Instituto requiere 1 (uno). El posible proveedor deberá entregar curriculum profesional en el que acredite que el Líder del Proyecto cuenta con dominio en el servicio solicitado, deberá acreditar 3 (tres) años de experiencia profesional como administrador de proyectos de la misma naturaleza que el objeto del presente procedimiento de contratación o servicios similares, así como 5 (cinco) años de experiencia profesional comprobable en el ramo de telecomunicaciones. El curriculum deberá incluir una descripción detallada de los proyectos en los que ha participado, nombre de la empresa o empresas donde laboró, período en el que laboró y datos del jefe inmediato superior con quien haya laborado. Del mismo modo deberá anexar la documentación académica probatoria referente al nivel licenciatura relacionada con las Tecnologías de Información y Comunicaciones (TIC) concluida y cédula profesional. Deberá entregar también copia simple de la certificación vigente del Project Management Institute como Project Management Professional (PMP) a nombre del Líder del proyecto, en el entendido que dicho certificado deberá estar vigente durante el período que abarque la contratación del servicio.
- Coordinadores del servicio: El Instituto requiere 1 (uno) Coordinador del servicio terrestre, 1 (uno)

Coordinador del servicio satelital y 1 (uno) Coordinador de centro de monitoreo. En este punto el posible proveedor deberá presentar por cada coordinador el curriculum profesional en el que acredite el domino del servicio a coordinar, el curriculum deberá incluir una descripción detallada de los proyectos en los que ha participado, nombre de la empresa o empresas donde laboró, período en el que laboró y datos del jefe inmediato superior con quien haya laborado. Del mismo modo deberá entregar la documentación académica probatoria referente al nivel licenciatura relacionada con las Tecnologías de Información y Comunicaciones (TIC) concluida y cédula profesional. Deberá entregar también copia simple de la certificación vigente en ITIL Foundation v3 a nombre del Coordinador del servicio terrestre, Coordinador del servicio satelital y Coordinador del centro de monitoreo, en el entendido que dichos certificados deberán estar vigentes durante el período que abarque la contratación del servicio.

- Personal para soporte a los sitios: En este punto el posible proveedor deberá presentar el curriculum profesional en el que acredite el domino del soporte a los sitios terrestres y satelitales, el curriculum deberá incluir una descripción detallada de los proyectos en los que ha participado, nombre de la empresa o empresas donde laboró, período en el que laboró y datos del jefe inmediato superior con quien haya laborado. Del mismo modo deberá entregar la documentación académica probatoria referente al nivel licenciatura relacionada con las Tecnologías de Información y Comunicaciones (TIC) concluida y cédula profesional, así como copia simple de certificaciones Cisco Certified Network Associate (CCNA) Routing and Switching, a favor de cuando menos cinco de los empleados que prestarán el soporte a los sitios terrestres y satelitales; en el entendido que dichos certificados deberán estar vigentes durante el período que abarque la contratación del servicio.

B. El posible proveedor deberá entregar copia simple del título de concesión vigente por parte de la SCT o de la autoridad competente para enlaces de comunicaciones. El título de concesión deberá contener como mínimo: El nombre y domicilio del concesionario, los servicios que podrá prestar el concesionario y la vigencia del mismo. **No presentar la documentación solicitada en este punto, es causal de desechamiento.**

C. El posible proveedor deberá entregar copia simple del permiso o autorización vigente, expedido por la autoridad correspondiente, con el cual demuestre que se proporcionará el servicio a través de un telepuerto autorizado *(telepuerto instalado y operado en el territorio Nacional)*, o en su defecto copia simple del permiso y/o contrato con el operador autorizado para operar el Telepuerto. **No presentar la documentación solicitada en este punto, es causal de desechamiento.**

D. El posible proveedor deberá entregar copia simple del certificado de homologación de los componentes de la Estación Terrena-Telepuerto, así como copia simple del certificado de homologación de los componentes de la Estación Terrena Remota-VSAT. **No presentar la documentación solicitada en este punto, es causal de desechamiento.**

E. Para lograr tiempos de respuesta óptimos y cumplir con los requerimientos de latencia mínimos solicitados por el Instituto en el anexo técnico, el posible proveedor deberá contar con la conexión directa de su POP de MPLS con el telepuerto de la solución satelital, por lo que deberá entregar la documentación que avale el tipo de conexión y el detalle de ancho de banda.

F. El posible proveedor deberá entregar manifestación escrita firmada por el representante legal de la empresa, en la que indique que el Centro de Monitoreo cumplirá con las especificaciones solicitadas en este anexo técnico, dicha manifestación deberá enlistar cada una de las especificaciones que deberá cumplir el Centro de Monitoreo.

G. El centro de monitoreo deberá ser provisto bajo el entorno de los siguientes estándares internacionales: ISO/IEC 20000-1:2011, ISO 9001:2008 o superior e ISO/IEC 27001:2005. El posible proveedor deberá entregar copia simple de dichas certificaciones, mismas que deberán estar vigentes.

H. El posible proveedor deberá entregar carta en papel membretado y firmada por el representante legal del fabricante de los equipos que integren la solución terrestre y satelital propuesta, en la cual detalle que el posible proveedor es distribuidor autorizado con capacidad de instalar y operar la infraestructura propuesta.

I. El posible proveedor deberá entregar documento en hoja membretada de la empresa la propuesta

técnica, mediante la cual acredite que oferta el servicio solicitado en el anexo técnico, mismo que deberá señalar de manera idéntica al anexo técnico, todas y cada una de las características, requisitos, bienes y servicios solicitados en el mismo, asimismo deberá contener la firma electrónica y/o autógrafa digitalizada del representante legal.

J. El posible proveedor deberá presentar copia simple de contratos debidamente formalizados, el posible proveedor deberá acreditar al menos 1 (uno) año de experiencia en la prestación de servicios iguales o similares al solicitado en el anexo técnico, los servicios descritos en los contratos deberán ser similares al objeto de éste proceso de contratación. Se entenderá por servicio similar aquel que provea de redes terrestres, redes satelitales y centro de monitoreo. Para este punto, el Instituto tomará como válidos a los contratos que en el objeto describan la prestación de alguno de los servicios descritos como similares, es decir, redes terrestres o redes satelitales o centro de monitoreo. Los contratos deberán haber sido celebrados con empresas, dependencias y/o entidades de la administración pública federal, no podrán tener fecha de firma anterior al año 2010 y no podrán tener una vigencia menor a 1(uno) año, se aceptará la presentación de contratos plurianuales. El posible proveedor deberá resaltar en los contratos: la vigencia, el número de contrato, objeto del contrato, resumen de servicios incluidos y cliente o beneficiario de los mismos. Asimismo el posible proveedor deberá anexar los nombres, correo electrónico y teléfonos del personal de contacto con los clientes de dicho contrato para efectos de verificación de la información proporcionada.

K. El posible proveedor deberá presentar copia simple de contratos debidamente formalizados, el posible proveedor deberá acreditar especialidad en la prestación de servicios similares al solicitado en el anexo técnico, los servicios descritos en los contratos deberán ser similares al objeto de éste proceso de contratación. Se entenderá por servicio similar aquel que provea de redes terrestres, redes satelitales y centro de monitoreo. Para este punto, el Instituto tomará como válidos a los contratos que en su objeto describan la prestación de los tres servicios descritos como similares, es decir, redes terrestres y redes satelitales y centro de monitoreo. Los contratos deberán haber sido celebrados con empresas, dependencias y/o entidades de la administración pública federal, no podrán tener fecha de firma anterior al año 2010 y no podrán tener una vigencia menor a 1 (uno) año, se aceptará la presentación de contratos plurianuales. El posible proveedor deberá resaltar en los contratos: la vigencia, el número de contrato, objeto del contrato, resumen de servicios incluidos y cliente o beneficiario de los mismos. Asimismo, el posible proveedor deberá anexar los nombres, correo electrónico y teléfonos del personal de contacto con los clientes de dicho contrato para efectos de verificación de la información proporcionada.

L. El posible proveedor deberá incluir en su proposición documento en hoja membretada de la empresa en el que indique la metodología, procesos y procedimientos que utilizará para prestar el servicio solicitado, éste documento deberá indicar la forma en la que el posible proveedor logrará técnicamente entregar el servicio a solicitado, el modelo que utilizará para el manejo de los diferentes perfiles que intervienen en sus procesos, la organización de su mesa de servicios, el proceso de atención a incidentes, así como la metodología, formatos y procedimientos que utilizará para medir en forma mensual la satisfacción del servicio que recibe el Instituto y las estrategias que llevará a cabo para lograr un proceso de mejora continua. No se aceptarán cartas bajo protesta de decir verdad en las que se comprometa el cumplimiento de cualquiera de las especificaciones del servicio.

M. El posible proveedor deberá incluir en su proposición documento en hoja membretada de la empresa en el que indique el modelo de matriz de escalación que utilizará para controlar el servicio que proporcionará al Instituto durante la vigencia del contrato, asimismo, la matriz de escalación deberá describir los tiempos definidos para la atención y solución a fallas en el servicio, incluyendo los medios de contacto electrónico, tales como correo electrónico y teléfonos tanto fijos como celulares.

N. El posible proveedor deberá incluir en su proposición en hoja membretada de la empresa la plantilla de los recursos humanos con los que cuenta para la prestación del servicio solicitado.

O. El posible proveedor deberá presentar copia simple de al menos 1 (uno) contrato de servicios similares al solicitado en el anexo técnico, se entenderá por servicio similar aquel que provea de redes terrestres, redes satelitales y centro de monitoreo. Los contratos deberán haber sido celebrados con empresas, dependencias y/o entidades de la administración pública federal, no podrán tener fecha de firma

ANEXOS

DIVISIÓN DE CONTRATOS

anterior al año 2010 y no podrán tener una vigencia menor a 1 (uno) año, se aceptará la presentación de contratos plurianuales. Los contratos deberán estar acompañados del documento que haga constar la cancelación de la garantía de cumplimiento respectiva, manifestación expresa de la contratante sobre el cumplimiento total de las obligaciones a cargo del posible proveedor o cualquier otro documento con el que se corrobore dicho cumplimiento, el contrato deberá estar debidamente concluido. En caso de presentar manifestación o cualquier otro documento con el que se corrobore el cumplimiento, deberá incluir el nombre, cargo, teléfono, correo electrónico, correo y rol del respectivo contrato, los servicios descritos en los contratos deberán ser similares al objeto de éste proceso de contratación, se entenderá por servicio similar aquel que provea de redes terrestres, redes satelitales, centro de monitoreo. El posible proveedor deberá resaltar en los contratos: la vigencia, el número de contrato, objeto del contrato, resumen de servicios incluidos y cliente o beneficiario de los mismos. Asimismo, el posible proveedor deberá anexar los nombres, correo electrónico y teléfonos del personal de contacto con los clientes de dicho contrato para efectos de verificación de la información proporcionada.

PARTIDA 2

Operbes S.A. de C.V. tomó en consideración la no entrega de los documentos conforme a lo establecido en el punto 8. Condiciones de Continuidad del presente documento.

No.	
1	Aceptación de la totalidad de los capítulos y secciones contenidos en este anexo técnico, para lo cual Operbes S.A. de C.V. empleará el mismo orden y secuencia de temas que comprende este 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 para evitar ambigüedades en la suscripción.
2	Descripción a alto nivel de la arquitectura global que Operbes S.A. de C.V. utilizará para prestar los servicios objeto de este anexo técnico, apegándose a la Arquitectura de Referencia definida en éste. Este documento describirá de forma general, las características de los componentes necesarios para entregar cada uno de los servicios administrados, pudiendo apoyarse para consolidar un documento concreto y conciso, en esquemas, diagramas, tablas, listados o cualquier elemento didáctico que el posible proveedor 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.
3	Descripción de la metodología, procesos, procedimientos y alianzas que Operbes S.A. de C.V. utilizará para la prestación de los servicios a contratar. Este documento hablará de la forma en la que Operbes S.A. de C.V. consolidará los diversos servicios, funcionalidades y tareas solicitadas en el Anexo Técnico a partir de sus métodos, mejores prácticas, alianzas comerciales y demás mecanismos de entrega de servicio.
4	Relación y descripción detallada de todos los Componentes Habilitadores, red de telecomunicaciones e Infraestructura Auxiliar que formarán parte de su solución para Operbes S.A. de C.V. descritos en el presente documento, en cualquiera de los elementos del Catálogo de Servicios correspondiente, conforme a lo establecido en este documento, que describan las características y especificaciones técnicas del fabricante de cada uno de ellos, para los casos en los que esto aplique. Las funcionalidades de estos servicios no deben ser referenciados a un catálogo de fabricante, no obstante, de conformidad a lo establecido en el anexo técnico, se incluirá y detallará.
5	Descripción detallada de cómo logrará Operbes S.A. de C.V., entregar los Servicios Administrados de Acceso a Internet, de acuerdo a cada una de las secciones comprendidas en el anexo técnico. Para construir este documento, Operbes S.A. de C.V. utilizará esquemas, descripciones de equipo y de software, métodos de integración de aplicaciones y hardware y cualquier elemento didáctico que considere conveniente para lograr una descripción lógica, comprensible y detallada de todos los Componentes Habilitadores, red de telecomunicaciones e Infraestructura Auxiliar.

6	Descripción detallada de cómo logrará Operbes S.A. de C.V. técnicamente, entregar todos y cada uno de los Servicios Operativos, de acuerdo a cada una de las secciones comprendidas en la sección del mismo nombre en el Anexo Técnico. Para construir este documento, Operbes S.A. de C.V. puede utilizar esquemas, descripciones de equipo y de software, métodos de integración de aplicaciones y hardware y cualquier elemento didáctico que considere conveniente para lograr una descripción lógica, comprensible y detallada.
7	Descripción del programa de Mantenimientos y Correctivos, y de los procedimientos, técnicas, prácticas y consideraciones que Operbes S.A. de C.V. ofrecerá para cubrir dichos servicios, de acuerdo a los Niveles de Servicio especificados en el presente documento. Deberá incluir, al menos: · La descripción de los procesos asociados a la labor · Los Recursos Humanos y Materiales involucrados · El tiempo definido para la atención de requerimientos y/o solución de fallas o los compromisos de acuerdo a los niveles de servicio solicitados en este documento · Los alcances técnicos del mantenimiento y los protocolos de prueba · Las rutas de escalamiento correspondientes
8	Descripción clara de cómo Operbes S.A. de C.V. proporcionará los Procesos de Administración de Problemas y los servicios de SOC, incluyendo las consideraciones técnicas de diseño, procedimientos y operación correspondientes, de acuerdo a lo especificado en las secciones dedicadas a estas solicitudes en el Anexo Técnico.
9	Manifestación escrita firmada por el Representante Legal de la empresa, en la que establezca que cuenta con las garantías y el soporte de los fabricantes de los Componentes Habilitadores de hardware y software, así como de los diferentes elementos de infraestructura auxiliar que incluya y que formen parte de la solución de los Servicios Administrados de Acceso a Internet, y que cuenta con personal calificado para efectuar el diseño, análisis, evaluación, operación, administración y mantenimiento de todos los servicios soportados por dichos Componentes Habilitadores y elementos activos.
10	Manifestación escrita firmada por el Representante Legal de la empresa, en la que establezca que cuenta con el personal calificado y debidamente certificado al más alto nivel por parte del fabricante de la solución tecnológica propuesta sobre los diferentes componentes activos (explícitamente abundará sobre: equipo CPE de Internet, clean pipes, componentes habilitadores y soluciones de seguridad, SOC) que formen parte de su solución para conducir las tareas de instalación, puesta en marcha, configuración, soporte, monitoreo y operación de los servicios objeto del anexo técnico.
11	Manifestación escrita firmada por el Representante Legal de la empresa, en la que ésta garantice específicamente la calidad de los trabajos y de los materiales menores a emplear en la instalación, a efectos de no presentar estos vicios ocultos al menos en la vigencia del contrato.
12	Manifestación escrita firmada por el Representante Legal de la empresa, en la que establezca con claridad que los equipos suministrados cuentan con las garantías solicitadas por parte de los fabricantes o distribuidores autorizados de los principales Componentes Habilitadores de Hardware y Software que integre a su solución.
13	Organigrama y currículo del personal inicial que será encargado de proporcionar el servicio contratado, de cara al IMSS. Operbes S.A. de C.V. incluirá hasta tres niveles (1-2-3) en el detalle top-bottom del organigrama, con la información requerida. Anexará a este entregable de su Propuesta Técnica, todos los currículos del personal de soporte certificado solicitado de manera obligatoria como parte del Anexo Técnico, indicando las certificaciones con las que cuenta y la fecha de obtención y caducidad del certificado en cuestión.
14	Operbes S.A. de C.V. dará cumplimiento a los niveles de servicio solicitados en el anexo técnico, para lo cual suscribirá como parte de su propuesta, las tablas con las métricas de nivel de servicio referidas, manifestando el compromiso explícito de dar cumplimiento a las mismas.
15	Entrega de documentos probatorios de experiencia, capacidades, habilidades y certificaciones del personal a cargo de los procesos del SOC, mediante la siguiente información: Copias de certificados vigentes, currículos actualizados, así como copia de las certificaciones solicitadas.

16	Manifestación escrita firmada por el representante legal de la empresa, donde exprese que Operbes S.A. de C.V. cuenta con un DRP (Disaster Recovery Plan, por sus siglas en inglés) para el respaldo de información crítica para la operación de los servicios. A la manifestación escrita, acompañará un documento técnico donde se explique dicho plan y cómo se vincula con los servicios específicos objeto de esta contratación.
17	Manifestación escrita, firmada por el representante legal de la empresa en el que manifieste que cuenta con al menos 5 años de experiencia en la provisión de servicios de SOC como los solicitados en esta contratación. El objetivo del requisito es demostrar al IMSS al menos cinco años de experiencia en proyectos relacionados con seguridad de información, para lo cual podrá acompañar copia simple de al menos un contrato que satisfaga la cantidad de tiempo expresada, junto con un resumen de éste, en el que se manifieste dicha experiencia de forma explícita.
18	Manifestación escrita firmada por el representante legal de la compañía, que indique que ésta cuenta con personal con certificación vigente en "ITIL Versión 3, nivel Expert y que la provisión y operación de los servicios objeto de esta contratación será debidamente realizada y supervisada por el personal que cuente con dicha certificación durante la vigencia del contrato (demostrando esta condición al menos para un recurso humano vinculado al servicio del IMSS). Operbes S.A. de C.V. incluirá de manera obligatoria, copia(s) de la(s) certificación(es), emitida por un organismo autorizado para realizar dicha certificación, donde pueda validarse a través de un número la vigencia de dicha certificación.
19	Manifestación escrita, firmada por el representante legal de la empresa en la cual especifica que cuenta con las alianzas necesarias con los fabricantes de las soluciones necesarias para el otorgamiento de los Servicios Administrados objeto del anexo técnico. **No presentar la documentación solicitada en este punto, es causal de desechamiento.**
20	Manifestación escrita firmada por el representante legal de la empresa, donde indique que cuenta con un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) que cumplan con los requisitos solicitados por el IMSS en el anexo técnico. Se adjuntará a dicha carta, un documento integral que con mucho detalle especifique la ubicación, procesos, certificaciones e infraestructura de dicho Centro de Operaciones de Seguridad.
21	Documento de propuesta del proceso de atención de problemas, alineada a las mejores prácticas establecidas en ITIL. Dicha propuesta contará, al menos, con los siguientes elementos: Clasificación de tipo de falla, tiempo de respuesta por tipo de falla, proceso de atención a falla, tiempo de resolución de falla.
22	Las áreas que brindarán el servicio de SOC al IMSS estarán certificadas en ISO/IEC 27001:2005. Operbes S.A. de C.V. entregará copia del documento de certificación que permita al IMSS vincular dicho proceso con el servicio solicitado en este anexo técnico y además, presentará una manifestación escrita firmada por el representante legal de la empresa en el que asegure contará con dicha certificación, anexando el documento probatorio, la entidad certificadora y su vigencia.
23	Manifestación por escrito, firmada por el representante legal de la empresa, 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.
24	Manifestación por escrito firmada por el representante legal de la empresa, en la que expresa que el personal encargado del diseño de la arquitectura de la solución tecnológica propuesta por los posibles proveedores acredita la certificación en PMI (certificado profesional en dirección de proyectos emitido por el Project Management Institute) o TOGAF (certificado en la Metodología y Herramientas para Desarrolar Arquitecturas en Empresas), incluyendo copia de la acreditación correspondiente.
25	Manifestación escrita, firmada por el representante legal de Operbes S.A. de C.V., en la que indique que su representada cuenta en su plantilla de personal con al menos cinco trabajadores con estudios a nivel licenciatura en carreras afines o relacionadas con la operación y administración de tecnologías de la información y comunicaciones. para la acreditación de este requisito deberán presentar las cédulas

	profesionales correspondientes certificadas por un notario público.
26	Manifestación escrita firmada por el Representante Legal de la empresa en la cual especifica que cuenta con las alianzas necesarias con los fabricantes de las soluciones necesarias para el otorgamiento de los servicios administrados objeto del anexo técnico. **No presentar la documentación solicitada en este punto, es causal de desechamiento.**

10. Condiciones técnicas de aceptación de los entregables.

PARTIDA 1

Operbes S.A. de C.V. tomó en consideración que este punto no aplica, ya que no está participando en esta partida (El proveedor está obligado a proporcionar el servicio solicitado a todos los sitios señalados en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual".

Para hacer constar que la prestación del servicio se llevó a cabo a entera satisfacción del Instituto, el proveedor deberá elaborar:

- Sitios terrestres: Protocolo de Pruebas para la Entrega de Sitios Terrestres Tipo A, (Apéndice 4).
- Sitios satelitales: Protocolo de Pruebas para la Entrega de Sitios Satelitales Tipo B, (Apéndice 5).

Ambos documentos se adjuntan al presente anexo y deberán ser entregados al Grupo Administrador del Contrato debidamente requisitados y firmados por el proveedor y por el Instituto).

PARTIDA 2

Entregables por Única Vez

Operbes S.A. de C.V. se compromete a entregar, de manera única a lo largo de la vigencia del contrato, un conjunto de documentos relacionados con su servicio. A continuación, se puntualizan los entregables mínimos para su mejor atención.

NÚMERO	NOMBRE Y DESCRIPCIÓN	LÍMITE DE ENTREGA
1	Matriz de Escalación	5 días naturales posteriores a la finalización de mesas de trabajo
2	Procedimiento de Control de Cambios	5 días naturales posteriores a la finalización de mesas de trabajo
3	Escrito del posible proveedor sobre las capacidades y habilidades para soportar los equipos.	45 días naturales posteriores a la notificación del fallo
4	Aseguramiento de Calidad en la Entrega	30 días naturales posteriores a la entrega del inmueble
5	Plan de trabajo nuevos inmuebles o reubicaciones	5 días naturales posteriores a la solicitud de cambio de inmueble o reubicaciones
6	Checklist de liberación del inmueble	5 días naturales posteriores a la migración del inmueble
7	Memorias Técnicas	10 días naturales posteriores a la entrega del inmueble
8	Procedimiento en caso de contingencia (Continuidad del Negocio)	30 días naturales posteriores a la firma del contrato
9	Plan de trabajo de transición de los servicios	2 meses antes de la finalización del contrato
10	Documentación generada en fase de migración	45 días naturales posteriores a la entrega del último inmueble
11	Categorizaciones para Mesa de Ayuda del IMSS	5 días naturales posteriores a la finalización

		de mesas de trabajo

Entregables Periódicos

A continuación, y como complemento a lo establecido en la sección anterior, se puntualizan aquellos entregables obligatorios bajo el criterio de entrega periódica, que serán elaborados y entregados al IMSS por Operbes S.A. de C.V.:

NUMERO	NOMBRE Y DESCRIPCION	FRECUENCIA DEL REPORTE
1	Operbes S.A. de C.V. entregará reportes de administración de configuraciones y cambios en la infraestructura, así como la actualización de una memoria técnica integral de los servicios.	Cada tres meses o cada vez que se efectúen cambios por alta, baja y cambio de nodo de la RPV
2	Disponibilidad, Latencia y Degradación por Pérdida de Paquetes, por sitio y por elemento funcional que forme parte de la solución. La información contenida será real sin sumarización o compactación, así como ser posible, para cada clase de servicio conforme a lo establecido anteriormente.	Se entregarán dentro de los primeros 5 días hábiles de cada mes
3.	Reporte de Atención y solución de fallas. Indicando los tipos de fallas, su tiempo medio de reparación (MTTR), si afectan o no la disponibilidad	Se entregarán dentro de los primeros 5 días hábiles de cada mes
4.	Disponibilidad, Latencia y Degradación por Pérdida de Paquetes del acceso a Internet, por sitio. La información contenida será real sin sumarización o compactación.	Se entregarán dentro de los primeros 5 días hábiles de cada mes
5.	Reporte ejecutivo. Contendrá estadísticas principales de uso y desempeño de todos los nodos.	Se entregará de manera anual, por periodos de 6 meses
6	Informes Ejecutivos por incidente. Este informe ejecutivo contendrá la descripción sencilla de la falla, sus causas y las acciones que se tomaron para resolverlas, el formato y la forma de entrega se definirá con Operbes S.A. de C.V. como parte de las reglas de operación. Sin embargo, el formato será electrónico.	Operbes S.A. de C.V. entregará a solicitud del IMSS, un reporte ejecutivo de los incidentes que considere críticos
7	Informes de gestión del SOC	Se entregarán dentro de los primeros 5 días hábiles de cada mes

Reportes en Línea

Operbes S.A. de C.V. tendrá disponibles, a lo largo de la vigencia del contrato, un conjunto de reportes en línea, mismos que puedan ser revisados por los funcionarios responsables del gobierno del servicio al interior del IMSS. A continuación, se puntualizan los entregables mínimos para su mejor atención. Se acordará en las Mesas de trabajo un tiempo con Operbes S.A. de C.V. en caso de ser el proveedor que resulte adjudicado, para poder adecuar la herramienta a sus necesidades específicas.

Tipo de Reporte	Descripción	Formato	Periodicidad
a) Reporte de salud	Muestra la salud de la red o grupo de elementos basados en la utilización y errores detectados. Permite verificar el desempeño actual e histórico de los elementos o grupos de elementos. Ver subreportes en seguida: Reportes de Excepciones. Reportes Resumidos Reportes -Top Ten	HTML, PDF, ASCII	Diario Semanal Mensual

Tipo de Reporte	Descripción	Formato	Periodos
	Reportes Detallados por Elemento Reportes Suplementarios.		
a.1) Reporte de salud: Excepciones	Permite determinar si un elemento en particular experimenta altos volúmenes, errores o errores repentinos Detalla la causa principal y despliega la tendencia de la condición; enlista las excepciones por prioridad.		
a.2) Reporte de salud: Resumen	Describe un resumen del rendimiento de los servicios utilizando cuatro gráficas: volumen total (sea en meses, semanas o días, anexando tablas de valores), volumen promedio, índice de salud promedio y situaciones a observar. Permite conocer tendencias y patrones regulares de tráfico en el tiempo.		
a.3) Reporte de salud: Top Ten	Muestra los enlaces más ocupados en la red administrada, basados en el volumen o índice de salud, así como los líderes en cambio tanto en volumen como en índice de salud.		
a.4) Reporte de salud Detallados por Elemento	Permite verificar el desempeño de cada circuito en la red. Ofrece comparativos de volumen contra la línea de base (4 semanas) o promedio histórico. Presenta el grado de ocupación de elementos por categorías mostradas en colores.		
b) Reporte detallado a la demanda	Muestra el rendimiento de los servicios durante un periodo de tiempo determinado, tomando en cuenta utilización de ancho de banda, bytes, frames, descartes, errores, disponibilidad, latencia y alcanzabilidad.	HTML, PDF, ASCII	Diario
c) Reporte de tendencias	Permite analizar el rendimiento de un servicio o conjunto de servicios sobre una variable (uso de ancho de banda, utilización de ancho de banda en horarios de operación de los inmuebles por ejemplo); así como identificar la causa de alguna degradación del rendimiento.	HTML, PDF, ASCII	Diario
d) Reporte de desglose de tráfico por protocolo en enlaces WAN	Reportado por medio de Cisco Network Based Application Recognition (Cisco NBAR), presenta el desglose de protocolos que cursan sobre el enlace durante el periodo solicitado. Operbes S.A. de C.V. integrará en su proposición cualquier herramienta para el reporte de tráfico por protocolo en enlaces WAN que cubra las características solicitadas, así como la funcionalidad y niveles de servicio solicitados.	HTML, PDF, ASCII	Diario
e) Monitoreo de niveles de servicio (SLA)	Herramienta para revisar en línea la disponibilidad del nodo y el retardo en los enlaces (Round Trip Time Delay). Capacidad de consultar de manera inmediata reportes de los 10 nodos con máximo RTT; disponibilidad promedio de los enlaces WAN y distribución de las disponibilidades de la red en categorías por colores.	HTML, PDF, ASCII	Diario

11.Cronograma de actividades

PARTIDA 1

Operbes S.A. de C.V. tomó en consideración que este cronograma de actividades no aplica de la partida 1, ya que se está participando por la partida 2.

ACTIVIDAD	MES							
	DURACIÓN	1	2	3	4	5	6	7
Mesas de trabajo para la continuidad del servicio.	7 días							
Entrega de certificados para el centro de monitoreo por parte del proveedor.	7 días							
Validación de operaciones del centro de monitoreo con el Instituto.	7 días							
Firma de Acuerdos de Nivel de Operación (OLAs) entre el	7 días							

Proveedor y los Terceros Involucrados con vigilancia del Grupo Administrador del Contrato del IMSS								
Prestación del servicio efectivo por parte del proveedor.	7 meses							

El Instituto brindará al proveedor un directorio general actualizado para brindar el soporte con los usuarios de sitio y/o coordinar visitas de servicio, el directorio contendrá: nombre del sitio, responsable de sitio, número telefónico de contacto, y correo electrónico del responsable.

PARTIDA 2

Operbes S.A. de C.V. considero el cronograma de actividades:

ID	HITO	MES					
		DURACIÓN	1	2	3	4	5
1	Mesas de trabajo para la continuidad del servicio.	7 días					
2	Firma de Acuerdos de Nivel de Operación (OLAs) entre el Proveedor y los Terceros Involucrados con vigilancia del Grupo Administrador del Contrato del IMSS	7 días					
3	Inicio de los Trabajos de Preparación para el Nuevo Servicio	A más tardar 2 meses antes del día de la Finalización del Contrato					
4	Prestación del servicio efectivo por parte del proveedor.	5 meses					

12. Niveles de servicio acordados que cumplirá

Operbes S.A. de C.V. tomó en consideración que los niveles de servicio no aplican de la partida 1, ya que se está participando por la partida 2.

PARTIDA 1

Servicio Administrado de Red Privada Virtual.

No.	SERVICIO	NIVEL
1	DISPONIBILIDAD DE ENLACES TERRESTRES.	98.89%
2	DISPONIBILIDAD DE ENLACES SATELITALES.	98.89%
3	DISPONIBILIDAD DE MESA DE SERVICIOS.	7X24X365

El porcentaje de disponibilidad está expresado en promedio mensual.

PARTIDA 2

Operbes S.A. de C.V. considero el nivel de disponibilidad de los servicios:

Servicio Administrado de Acceso a Internet.

Tipo de Nivel de Servicio	Descripción	Nivel Comprometido
Disponibilidad	Disponibilidad de los Servicios Administrados de Acceso a Internet (por Nodo)	99.98%
Disponibilidad	Disponibilidad del Servicio de Prevención de Intrusos (IPS)	99.96%
Disponibilidad	Disponibilidad del Servicio de Firewall en Alta Disponibilidad	99.96%
Disponibilidad	Disponibilidad del Servicio de Análisis de Flujo	99.96%
Disponibilidad	Disponibilidad del Servicio de Control de Acceso a Páginas Web	99.96%
Disponibilidad	Disponibilidad del Servicio de Análisis de Vulnerabilidades	99.96%

Disponibilidad	Disponibilidad del Servicio de Proxy	99.96%
Entrega	Entrega de modificaciones en Ancho de Banda de Internet	95% de las veces en 4 horas o menos
Desempeño	Latencia	Menor a 100 milisegundos de ida y vuelta al Punto de Acceso a la Red más cercano

13.Requerimientos de arquitectura tecnológica

Operbes S.A. de C.V. tomó en consideración que este no punto aplica, porque son servicios de la partida 1 en la cual Operbes S.A. de C.V. no participa.

El servicio deberá integrar la interconexión con el Sitio Nube IMSS Digital (también conocido como Punto Neutro), ubicado en Santa Fe, con la red MPLS, en la que se integran los enlaces de los sitios señalados en el "Apéndice 1: Inventario de Nodos para el Servicio Administrado de Red Privada Virtual"; así como en los sitios que el Instituto designe, para lo cual el posible proveedor deberá utilizar los enlaces con capacidad de 200 Mbps de forma sumarizada.

El posible proveedor deberá suministrar los equipos de ruteo requeridos para soportar la interconexión solicitada en el párrafo anterior, así como los servicios de configuración y puesta a punto de la mencionada interconexión.

14.Restricciones e interfaces con otros elementos

Operbes S.A. de C.V. tomó en consideración que no aplica

15.Causales de desechamiento.

Operbes S.A. de C.V. tomó en consideración que deberá referirse al incumplimiento de los puntos las señaladas en el numeral 6. Perfil del posible proveedor del presente anexo técnico.

16.Formato de declaración de no conflicto de interés.

Operbes S.A. de C.V. tomó en consideración que, con base en lo indicado en las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto, punto 4 Políticas, apartado 4.15, inciso i, se anexa al presente el Anexo 4, Declaración de no conflicto de interés.

17.Relación de Anexos

Operbes S.A. de C.V. tomó en consideración la relación de anexos para la partida 2.

Id	Nombre	Descripción	Fecha de integración al proyecto
SGMP TRA 01	Apéndice 1	Inventario de Nodos para el Servicio Administrado de Red Privada Virtual.	28/05/2020
SGMP TRA 02	Apéndice 2	Inventario de Nodos para el Servicio Administrado de Acceso a Internet.	28/05/2020
SGMP TRA 03	Apéndice 3	Cobertura de la Red de Telecomunicaciones del posible proveedor para los Enlaces de Internet	28/05/2020
SGMP TRA 04	Apéndice 4	Protocolo de Pruebas para la Entrega de Sitios Terrestres "Tipo A"	28/05/2020
SGMP TRA 05	Apéndice 5	Protocolo de Pruebas para la Entrega de Sitios Satelitales "Tipo B"	28/05/2020
SGMP TRA 06	Apéndice 6	Declaración de no conflicto de interés	28/05/2020
SGMP TRA 07	TC	Términos y Condiciones	28/05/2020

ANEXOS
DIVISIÓN DE CONTRATOS

19

SIN TEXTO

Bestel.

.com.mx

Sección I "Precios Unitarios" , PARTIDA 2

Instituto Mexicano del Seguro Social
Dirección de Innovación y Desarrollo Tecnológico (DIDT)

A	B	C	D	E	F	G
No	Conceptos del Servicio	Mínimo	Máximo	Precio Unitario (Mensual)	Importe Mínimo	Importe Máximo
1	Servicios Administrados de Acceso a Internet para Nodo "Nube IMSS Digital"	1	1	$323,500.00	$323,500.00	$323,500.00
2	Servicios Administrados de Acceso a Internet para Nodo "CeNaTI DF"	1	1	$323,500.00	$323,500.00	$323,500.00
3	Servicios Administrados de Seguridad de Internet para el Nodo "CeNaTI DF"	1	1	$1,355,099.50	$1,355,099.50	$1,355,099.50
4	Servicios Administrados de Acceso a Internet para Nodo "CeNaTI Monterrey"	1	1	$323,500.00	$323,500.00	$323,500.00
5	Servicios Administrados de Seguridad de Internet para el Nodo "CeNaTI Monterrey"	1	1	$1,355,099.50	$1,355,099.50	$1,355,099.50
6	Servicio de Incremento de Ancho de Banda en Internet	950	2,375	$1.00	$950.00	$2,375.00
					$3,681,649.00	$3,683,074.00
					$589,063.84	$589,291.84
					$4,270,712.84	$4,272,365.84

	INSTRUCCIONES PARA EL LLENADO DE LA SECCIÓN I: PRECIOS MÁXIMOS DE REFERENCIA UNITARIOS
1	El participante deberá indicar como parte de su propuesta económica al RFP, los precios unitarios que decida otorgar en cada concepto escribiéndolos en la columna "E". Estos precios unitarios deberán estar redondeados a dos decimales, en todos los casos deberán ser mayores a cero y no podrán quedar en blanco.
2	Para determinar el alcance de cada uno de los conceptos mencionados en la columna "B", el participante deberá considerar la definición de cada uno de ellos de acuerdo a lo descrito en el anexo técnico.
3	El archivo de manera automática indicará en la columna "F" el importe mínimo de cada concepto.
4	El archivo de manera automática indicará en la columna "G" el importe máximo de cada concepto.
5	La volumetría que se proporciona en las columnas "C" y "D" es exclusivamente para efectos de cotización y no necesariamente reflejan los requerimientos del Instituto, por lo que dichas cantidades no se deberán considerar como las cantidades a contratar. Cada participante deberá cotizar precios unitarios por cada uno de los conceptos establecidos. El contrato que resulte de este proceso de contratación será abierto y los servicios serán solicitados bajo demanda, la cantidad de servicios a contratar se determinará por el presupuesto mínimo y máximo establecido.
6	El archivo calculará de manera automática las suma resultante de la columna "F" en la celda correspondiente al "Subtotal", indicando el importe mínimo de la propuesta económica del participante.
7	El archivo calculará de manera automática las suma resultante de la columna "G" en la celda correspondiente al "Subtotal", indicando el importe máximo de la propuesta económica del participante.
8	Las únicas celdas en las que se espera algún valor de parte del licitante, se han sombreado en color gris, columna "E".
9	No se deberá integrar en ningún precio unitario componentes de costo distintos a los definidos para dicho servicio en el anexo técnico
10	Esta Sección debidamente llenada de acuerdo con estas instrucciones, deberá ser incorporado por el participante como parte de su Respuesta al RFP, tanto de forma impresa -debidamente firmado al pie del mismo, donde se indica- como de manera digital, usando como base este mismo archivo.
	Todos los precios que aparecen en esta sección son sin I.V.A. **Los participantes deberán ingresar la siguiente información en el formato:**

Vigencia de la oferta: (expresar al menos 90 días naturales)	**90 DIAS NATURALES**
Precios firmes durante la vigencia del contrato, expresados	**PRECIOS EXPRESADOS EN PESOS MEXICANOS**
Nombre de la empresa participante	**BESTEL (OPERBES S.A.DE C.V.)**
Nombre del Representante Legal de la empresa participante	**LUIS ALBERTO DE LA GARZA AGUIRRE**

Atentamente

LUIS ALBERTO DE LA GARZA AGUIRRE
Director Ejecutivo Gobierno y Representante Legal
OPERBES, S.A. DE C.V.

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

Acta de Adjudicación

Adjudicación Directa Nacional número AA-050GYR019-E132-2020

En la Ciudad de México, siendo las **16:00 horas del día 07 de agosto del 2020,** en la sala de juntas de la División de Contratación de Activos y Logística; ubicada en la Calle Durango número 291, Quinto Piso, Colonia Roma Norte, Código Postal 06700, Demarcación Territorial Cuauhtémoc, presente el servidor público cuyo nombre y firma aparecen al final del presente documento, con objeto de llevar a cabo la Adjudicación Directa Nacional número **AA-050GYR019-E132-2020, para la contratación del "Servicio de Comunicación para Enlaces de Criticidad Media y Normal del IMSS, Partida 2.- Servicio Administrado de Acceso a Internet",** requerido por el Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional, mediante oficio número **09 52 76 61 5300/2020000545** conforme con lo siguiente: ----------

---

Adjudicación ----------

Derivado del Acuerdo número **AC-39/SO-07/2020**, mediante el cual el Comité de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social, en la **Sesión Ordinaria Número 07/2020,** celebrada el 31 de julio del 2020, con fundamento en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 3 fracción IX, 22 fracción II, 26 fracción III, 26 Bis fracción I, 28 fracción I, 40, 41 fracción III y 46 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP) así como 71, y 72 fracción III y 85 de su Reglamento, resuelve dictaminar favorablemente por unanimidad la excepción a la Licitación Pública, mediante el procedimiento de Adjudicación Directa para la contratación de los "**Servicio de Comunicación para Enlaces de Criticidad Media y Normal del IMSS, Partida 2.- Servicio Administrado de Acceso a Internet".** El monto adjudicado es por la cantidad de **$29'906,560.88 (veintinueve millones novecientos seis mil quinientos sesenta pesos 88/100 M.N.)**, incluyendo el Impuesto al Valor Agregado (IVA), para ello se cuenta con el Dictamen de Disponibilidad Presupuestal número **0000187152-2020** (Se anexa copia del formato CAAS 01 como parte integrante del presente documento). ----------

---

Atendiendo a lo anterior, de conformidad con el artículo 37 fracción IV de la LAASSP y considerando que de esta forma se aseguran las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes para el Instituto se adjudica a la empresa **Operbes, S.A. de C.V.**, el ejercicio del monto adjudicado deberá guardar estrecha relación conforme a los precios unitarios ofertados en la propuesta económica del proveedor, la cual se da por reproducida en esta parte como si a la letra se insertara, misma que **se anexa** y de la que se destaca el siguiente resumen: ----------

---

A	B	C	D	E	F	G
No	Conceptos del Servicio	Mínimo	Máximo	Precio Unitario (Mensual)	Importe Mínimo	Importe Máximo
1	Servicios Administrados de Acceso a Internet para Nodo "Nube IMSS Digital"	1	1	$323,500.00	$323,500.00	$323,500.00
2	Servicios Administrados de Acceso a Internet para Nodo "CeNaTI DF"	1	1	$323,500.00	$323,500.00	$323,500.00
3	Servicios Administrados de Seguridad de Internet para el Nodo "CeNaTI DF"	1	1	$1,355,099.50	$1,355,099.50	$1,355,099.50
4	Servicios Administrados de Acceso a Internet para Nodo "CeNaTI Monterrey"	1	1	$323,500.00	$323,500.00	$323,500.00
5	Servicios Administrados de Seguridad de Internet para el Nodo "CeNaTI Monterrey"	1	1	$1,355,099.50	$1,355,099.50	$1,355,099.50
6	Servicio de Incremento de Ancho de Banda en Internet	950	2,375	$1.00	$950.00	$2,375.00
				Subtotal	$3,681,649.00	$3,683,074.00
				IVA	$589,063.84	$589,291.84
				Total	$4,270,712.84	$4,272,365.84

ANEXOS
DIVISIÓN DE CONTRATOS

Acta de Adjudicación

Adjudicación Directa Nacional número AA-050GYR019-E132-2020

De la consulta a la información publicada en el Sistema Electrónico de Información Pública Gubernamental, denominado "CompraNet", sobre proveedores y contratistas sancionados, multados, inhabilitados así como con el impedimento para presentar propuestas o celebrar contratos no se encontró al proveedor arriba indicado. ----------

---

El servicio deberá prestarse de conformidad con los términos y condiciones y anexo técnico emitidos por el área requirente que rigen la presente contratación y tendrá una vigencia a partir del día hábil siguiente al de la adjudicación y hasta el 31 de diciembre de 2020. ----------

---

De conformidad con el artículo 37 fracción V de lá LAASSP, se notifica al proveedor, que la firma del contrato se realizará a más tardar el día **21 de agosto de 2020**, en la División de Contratos, sita en la Calle Durango número 291, décimo piso, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, Ciudad de México, en horario de 9:30 a 14:00 y de 16:00 a 18:00 horas, lo anterior de conformidad a lo establecido en el artículo 46 de la LAASSP. Para tal fin deberá de entregar previamente copia y presentar original para cotejo en la División de Contratos de los siguientes documentos: ----------

---

Para la firma del contrato deberá presentar los siguientes documentos: ----------

Persona moral: ----------

a) Acta constitutiva y, en su caso, sus respectivas modificaciones. ----------

b) Poder notarial del representante legal que firmará el contrato. ----------

c) Identificación oficial vigente y con fotografía del representante legal. ----------

d) Cédula de Registro Federal de Contribuyentes. ----------

e) Comprobante de domicilio con vigencia no mayor a 3 meses. ----------

f) En su caso, escrito de estratificación de empresa en términos del artículo 3 de la Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa. ----------

g) Escrito en términos del artículo 50 y 60 de la LAASSP. ----------

h) Escrito bajo protesta de decir verdad que no desempeña empleo, cargo o comisión en el servicio público, o en su caso que, a pesar de desempeñarlo, con la formalización del contrato correspondiente no se actualiza un conflicto de interés. (Ley General de Responsabilidades Administrativas DOF 18-07-2016). ----------

i) Opinión positiva de cumplimiento de obligaciones fiscales emitida por el SAT vigente a la firma del contrato, en términos del artículo 32-D del Código Fiscal de la Federación. ----------

j) Opinión positiva de cumplimiento de obligaciones en materia de seguridad social vigente a la firma del contrato emitida por el IMSS, en términos del artículo 32-D del Código Fiscal de la Federación y del Acuerdo ACDO.SA1.HCT.101214/281.P.DIR publicado en el DOF el 27 de febrero de 2015. ----------

k) Constancia vigente de situación fiscal emitida por el Instituto del Fondo Nacional de la Vivienda para los Trabajadores (INFONAVIT) en los términos establecidos por las "Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y

Acta de Adjudicación

Adjudicación Directa Nacional número AA-050GYR019-E132-2020

entero de amortizaciones" publicadas en el Diario Oficial de la Federación (DOF) el 28 de junio del 2017. ----------

---

En caso de que el licitante: ----------

a) No se encuentre registrado ante este instituto o; ----------

b) Cuente con Registro Patronal, pero se encuentre dado de baja o; ----------

c) No tenga personal que sea sujeto de aseguramiento obligatorio, de conformidad con lo dispuesto por el artículo 12 de la LSS. ----------

---

No podrá obtener la citada Opinión, por lo cual dicho licitante podrá dar cumplimiento a tal requerimiento presentando lo siguiente: ----------

---

I. Documento emitido por este Instituto (resultado de la consulta en el sistema para obtener la Opinión), en el que se haga constar que no se puede emitir la Opinión de cumplimiento, de conformidad con la Regla Quinta del Anexo único del ACDO.SAI.HCT.101214/281.P.DIR; ---------

---

II. Escrito libre, bajo protesta de decir verdad, que no le es posible obtener la multicitada Opinión, justificando el motivo y anexando el documento en el que conste que no se puede emitir la misma y; ----------

---

III. En el caso de que el licitante manifieste que presta sus servicios a través de trabajadores subcontratados con un tercero, deberá de presentar en tal caso, junto con la documentación citada en los dos párrafos anteriores, la Opinión de cumplimiento de obligaciones del subcontratante, desde luego, vigente y positiva (lo anterior en términos del artículo 15-A de la LSS). ----------

---

En caso de que el licitante no cuente con trabajadores debido a que celebró contrato de prestación de servicios con otra empresa que es la que tiene contratados a los trabajadores (outsourcing), deberá presentar dicho contrato, así como escrito libre en el que manifieste que no se encuentra obligado debido a tal situación y opinión positiva vigente de cumplimiento de obligaciones en materia de seguridad social de la empresa subcontratada emitida por el IMSS. ----

---

En caso de que el participante forme parte de un grupo comercial y uno de los entes que forma parte del grupo se encarga de administrar la plantilla laboral de todas las empresas que lo conforman, será necesario que exhiba el documento que acredite la subcontratación para situarse en el supuesto del párrafo anterior. ----------

---

En caso de que el participante no cuente con trabajadores, deberá presentar escrito libre en el que manifieste que no se encuentra obligado a inscribirse ante el IMSS, por lo que no puede obtener la opinión de cumplimiento de obligaciones en materia de seguridad social. ----------

---

ANEXOS
DIVISIÓN DE CONTRATOS

Acta de Adjudicación

Adjudicación Directa Nacional número AA-050GYR019-E132-2020

Para los casos de contratos que se formalicen con personas físicas que presten sus servicios por sí mismos y por lo tanto no cuentan con un Registro Patronal ni tengan trabajadores registrados en el Instituto, el particular deberá de manifestar mediante escrito libre, bajo protesta de decir verdad, que no le es posible obtener la multicitada Opinión, justificando el motivo y anexando el documento (resultado de la solicitud de Opinión que le da el Sistema institucional) en el que conste que no se puede emitir la misma. ----------

---

En el caso de aquellos patrones (proveedores o contratistas y sus subcontratados) que tengan más de un Registro Patronal ante el Instituto y alguno o más de uno de estos Registros no se encuentre al corriente en el cumplimiento de las multicitadas obligaciones, no se podrá considerar que se encuentra al corriente en el cumplimiento de dichas obligaciones, aun cuando el registro patronal que haya utilizado para el contrato que se trate si se encuentre al corriente en sus pagos, por lo que deberá regularizar todos sus Registros a efecto de poder obtener la Opinión positiva. ----------

---

En caso de que el participante cuente con trabajadores contratados bajo el régimen de honorarios asimilados a salarios, deberá presentar el(los) contrato(s) con los que acredite el régimen de contratación, así como escrito libre en el que manifieste que no se encuentra obligado a inscribirse ante el IMSS debido a tal situación, por lo que no puede obtener la opinión de cumplimiento de obligaciones en materia de seguridad social. ----------

---

En caso de que el licitante se encuentre inscrito en el Registro Único de Proveedores y Contratistas de CompraNet, deberá remitir únicamente la documentación referida en los **incisos h), i) j) y k).** --

---

Asimismo, de conformidad con el artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y de la fracción III del artículo 85 de su Reglamento se informa a la empresa adjudicada que deberán entregar la Garantía de Cumplimiento de Contrato dentro de los diez días naturales posteriores a la firma del mismo ----------

---

De conformidad con el artículo 37 fracción VI de la LAASSP, así como con el numeral 5.3.8 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social y el numeral 7.1.3.2.2.3., del Manual de Organización de la Dirección de Administración este Acto es presidido por el Ingeniero Vicente Callejas Serrano, Titular de la División de Contratación de Activos y Logística, de la Coordinación Técnica de Adquisición, de Bienes de Inversión y Activos de la Coordinación de Adquisición de Bienes y Contratación de Servicios. ----------

---

No existiendo otro asunto que tratar, se da por terminado este procedimiento a las **18:30 horas** del día de su fecha de inicio, esta acta consta de **5 (cinco) hojas**, adjuntándose como parte integrante de la misma **1 (una) hoja del Formato CAAS 01 y 1 (una) hoja de propuesta económica,** por lo que se rubrica al margen y firma al calce para la debida constancia de notificación de la misma y efectos legales procedentes, la persona que interviene en todas y cada una de las hojas que integran el acta. ----------

Acta de Adjudicación

Adjudicación Directa Nacional número AA-050GYR019-E132-2020

Por el Instituto Mexicano del Seguro Social:

Titular de la División de Contratación de Activos y Logística (Área Contratante)	**Vicente Callejas Serrano**

Por la empresa **Operbes, S.A. de C.V.:**

Representante Legal	**Luis Alberto de la Garza Aguirre**

La firma que antecede corresponde al procedimiento de contratación que se realiza mediante la Adjudicación Directa Nacional número **AA-050GYR019-E132-2020**, **para la contratación del "Servicio de Comunicación para Enlaces de Criticidad Media y Normal del IMSS, Partida 2.- Servicio Administrado de Acceso a Internet".**

Fin del Acta

Recibí copia
Luis Alberto de la Garza A.
07/ago/2020

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

INSTITUTO MEXICANO DEL SEGURO SOCIAL
COMITÉ DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS

FORMATO CAAS 01

ASUNTO: Solicitud de dictamen sobre la procedencia de excepción al procedimiento de Licitación Pública para llevar a cabo la contratación del "Servicio de Comunicación para Enlaces de Criticidad Media y Normal del IMSS, Partida 2.- Servicio Administrado de Acceso a Internet", por un importe total de $29,906,560.88 (veintinueve millones novecientos seis mil quinientos sesenta pesos 88/100 M.N.) IVA incluido, la vigencia del servicio será a partir del día siguiente a la notificación de la adjudicación y hasta el 31 de diciembre de 2020.

SESIÓN No. 07/2020

ORDINARIA X EXTRAORDINARIA

DÍA 31 MES 07 AÑO 2020.

CANTIDAD Y DESCRIPCIÓN DE LOS BIENES O SERVICIOS	MOTIVACIÓN Y FUNDAMENTACIÓN	ACUERDO AC-39/SO-07/2020
"Servicio de Comunicación para Enlaces de Criticidad Media y Normal del IMSS, Partida 2.- Servicio Administrado de Acceso a Internet"	Artículos 134 de la Constitución Política de los Estados Unidos Mexicanos, 3 fracción IX, 22 fracción II, 26 fracción III, 40 y 41 fracción III de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público (LAASSP), así como 71, 72 fracción III y 85 de su Reglamento. En virtud de acreditar el supuesto de Ley consistente en evitar pérdidas o costos adicionales importantes cuantificados y justificados.	**El Comité Resuelve:** **Dictamina favorablemente por unanimidad, la excepción a la licitación pública para llevar a cabo la contratación del servicio.**

CONTRATO ABIERTO (Artículo 47)	NO	DICTAMEN DE DISPONIBILIDAD PRESUPUESTAL	120	MONTO:	**Total $29,906,560.88 pesos.**
ABASTO SIMULTÁNEO (Artículo 59)	NO	PRECIOS SUJETOS A AJUSTE	NO	LUGAR DE ENTREGA:	ANEXO 2
CONTRATO PLURIANUAL (Artículo 25)	NO	TRATADOS DE LIBRE COMERCIO	NO	CONDICIONES DE ENTREGA:	ANEXO 2

DIRECCIÓN DE FINANZAS VOCAL SUPLENTE	DIRECCIÓN DE PRESTACIONES MÉDICAS VOCAL SUPLENTE	DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO VOCAL SUPLENTE
PRESIDENTE		COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS VOCAL

LIC. RAFAEL RICARDO SÁNCHEZ RAMOS
SECRETARIO TÉCNICO

ANEXOS

DIVISIÓN DE CONTRATOS

SIN TEXTO

ANEXO 3 (TRES)

"DOCUMENTO DE DESIGNACIÓN DE ADMINISTRADOR DEL CONTRATO"

ANEXOS

DIVISÍON DE CONTRATOS

EL PRESENTE ANEXO CONSTA DE **02** HOJAS INCLUYENDO ESTA CARÁTULA

SIN TEXTO

Oficio N° 09 52 76 61 5300/2020000**538**

Ciudad de México, a 31 de julio de 2020

Lic. Leonardo Alvarado Velázquez
Coordinador de Servicios
Administrativos de la DIDT
P r e s e n t e

Con relación al inicio del procedimiento de contratación del ***"Servicio de Comunicación para Enlaces de Criticidad Media y Normal del IMSS, Partida 2.- Servicio Administrado de Acceso a Internet"*** para el ejercicio 2020.

Al respecto y a efecto de atender de manera oportuna las necesidades en materia de Tecnología de la Información y Comunicaciones del Instituto Mexicano del Seguro Social, les informo que el suscrito, C. Ing. Eduardo Oropeza Ortiz, con cuenta de correo electrónico: eduardo.oropeza@imss.gob.mx y teléfono 5238-2700, extensión 11911, fungirá como **"Administrador del Contrato"**, con fundamento en lo dispuesto por los artículos 2 fracción V, 74, y 84 del Reglamento Interior del Instituto Mexicano del Seguro Social; numeral 4.17 y 5.3.15 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social, y conforme a lo previsto en el numeral 7.1.2., del Manual de Organización de la Dirección de Innovación y Desarrollo Tecnológico vigente, así como el "*ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias*, publicado en el Diario Oficial de la Federación el 23 de julio de 2018.

Sin otro particular por el momento, hago propicia la ocasión para enviarles un cordial saludo.

Atentamente,

Ing. Eduardo Oropeza Ortíz
Coordinador de Sistemas de Infraestructura
Tecnológica Institucional adscrito a la DIDT

ANEXOS
DIVISIÓN DE CONTRATOS

EOO/jom/rvm

SIN TEXTO