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

CONTRATO ABIERTO PLURIANUAL PARA LA PRESTACIÓN DE LOS "SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024" (PARTIDA 1), QUE CELEBRAN, POR UNA PARTE, EL INSTITUTO MEXICANO DEL SEGURO SOCIAL, REPRESENTADO POR EL **MTRO. ZOÉ ALEJANDRO ROBLEDO ABURTO, EN SU CARÁCTER DE DIRECTOR GENERAL,** EN ADELANTE **"EL INSTITUTO"** Y, POR LA OTRA, LA EMPRESA DENOMINADA **OPERBES, S.A. DE C.V.**, (EL PARTICIPANTE A) REPRESENTADA POR LOS **C.C. LUIS ALBERTO DE LA GARZA AGUIRRE** Y **CESAR GERÓNIMO JIMÉNEZ CERVANTES**, EN SU CARÁCTER DE REPRESENTANTES LEGALES, EN PARTICIPACIÓN CONJUNTA CON **SILENT4BUSINESS, S.A. DE C.V.** (EL PARTICIPANTE B), REPRESENTADA POR EL **C. GERARDO GARIBAY AYMES**, EN SU CARÁCTER DE REPRESENTANTE LEGAL Y **BUFETE EMPRESARIAL GTI, S.A. DE C.V.** (EL PARTICIPANTE C), REPRESENTADA POR EL **C. JUAN LUIS PINEDA GONZÁLEZ**, EN SU CARÁCTER DE REPRESENTANTE LEGAL, A QUIENES EN FORMA CONJUNTA O INDIVIDUALMENTE SE LES DENOMINARÁ EN LO SUCESIVO **"EL PROVEEDOR"** Y EN FORMA CONJUNTA CON **"EL INSTITUTO"**, SE LES DENOMINARÁ **"LAS PARTES"**, AL TENOR DEL ANTECEDENTE, DECLARACIONES Y CLÁUSULAS SIGUIENTES:

## A N T E C E D E N T E

**Único.** La presente contratación es el resultado del procedimiento de Licitación Pública Nacional Electrónica número **LA-050GYR019-E182-2022**, realizada al amparo de lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos y en los artículos 26 fracción I, 26 Bis fracción II, 27, 28 fracción I y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y los correlativos de su Reglamento, y en términos del Acta de Fallo de 4 de octubre de 2022, suscrita por la Titular de la División de Contratación de Activos y Logística dependiente de la Dirección de Administración de "**EL INSTITUTO**", documento que se agrega en el **Anexo 3 (tres)** del presente contrato.

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

**I.** **"EL INSTITUTO"** declara, a través de su Director General, 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 Mtro. Zoé Alejandro Robledo Aburto, se encuentra facultado para suscribir el presente instrumento jurídico en representación de **"EL INSTITUTO",** con fundamento en los artículos 268 fracción III y 277 F, párrafo cuarto, de la Ley del Seguro Social y 66, fracciones I y XVI del Reglamento Interior del Instituto Mexicano del Seguro Social, y

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se pronuncia sobre la procedencia y/o viabilidad de los aspectos técnicos, económicos y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con base en el dictamen elaborado por la División de Dictamen Jurídico de Contratos y Convenios, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número: DC/DDJCC/ADQ/2022/007

GOBIERNO DE MÉXICO | IMSS



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

acredita su personalidad mediante el testimonio del acta pública número 74,291 de 3 de julio de 2019, pasada ante la fe del licenciado Ignacio Soto Sobreyra y Silva, titular de la Notaría Pública número 13 de la Ciudad de México, en la que consta la protocolización de su nombramiento como Director General de **"EL INSTITUTO"**, para celebrar, en forma indelegable, contratos plurianuales, cuya prestación genere una obligación de pago para **"EL INSTITUTO"**, igual o mayor a 190,150 veces la Unidad de Medida y Actualización (UMA), en alguno de sus años de vigencia, 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.

Su nombramiento como Director General de **"EL INSTITUTO"**, quedó inscrito en el Registro Público de Organismos Descentralizados, bajo el folio 97-5-19062019-180811, de 19 de junio de 2019, en cumplimiento a lo ordenado en el artículo 25, fracción III, de la Ley Federal de las Entidades Paraestatales.

**I.4** De conformidad con el artículo 84, penúltimo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, suscribe el presente instrumento el C. Abraham Gutiérrez Castillo, Titular de la División de Seguridad Informática Física, con R.F.C [redacted] facultado para administrar el cumplimiento de las obligaciones que deriven del objeto del presente contrato, quien podrá ser sustituido en cualquier momento en su cargo o funciones, bastando para tales efectos un comunicado por escrito y firmado por el servidor público facultado para ello, dirigido al representante de **"EL PROVEEDOR"** para los efectos del presente contrato, encargados del cumplimiento de las obligaciones contraídas en el presente instrumento jurídico.

**I.5** **"EL INSTITUTO"** cuenta con recursos suficientes y con autorización para ejercerlos en el cumplimiento de sus obligaciones derivadas del presente contrato, como se desprende del Dictamen de Disponibilidad Presupuestal Previo con cuenta número 42062493, con número de folio 0000439264-2022, de fecha 6 de octubre de 2022, emitido por la Titular de la División de Control y Seguimiento al Presupuesto de Operación en Ámbito Central, documento que se agrega al presente contrato en el **Anexo 1 (uno)**.

**I.6** De conformidad con el artículo 277 F, párrafo primero, de la Ley del Seguro Social, el Consejo Técnico de **"EL INSTITUTO"** autorizó llevar a cabo la contratación plurianual, de los Servicios Administrados de Seguridad Informática y Comunicaciones y el presupuesto a ejercer, conforme al Acuerdo número ACDO.AS3.HCT.271021/266.P.DIDT, emitido el día 27 de octubre de 2021 por el citado Órgano de Gobierno, documento que se agrega al presente contrato en el **Anexo 1 (uno)**.

**I.7** Para efectos fiscales las Autoridades Hacendarias le han asignado el Registro Federal de Contribuyentes **N° IMS421231I45**.

**I.8** Tiene establecido su domicilio en Calle Durango número 291, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, en la Ciudad de México, mismo que señala para los fines y efectos legales del presente contrato.

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con base en el dictamen elaborado por la División de Dictamen Jurídico de Contratos y Convenios, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número DC/DDJCC/ADQ/2022/007

La validación jurídica se efectúo sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se pronuncia sobre la procedencia y/o viabilidad de los aspectos técnicos, económicos y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

GOBIERNO DE MÉXICO

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: RFC, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN I Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016

**II.- "EL PROVEEDOR"** declara, a través de sus Representantes Legales, que:

**OPERBES, S.A. DE C.V.**, (El Participante A)

**II.1** Es una persona moral legalmente constituida 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 la Municipalidad de Tlaquepaque, Jalisco, e inscrita en el Registro Público de la Propiedad y de Comercio de la misma Entidad, en el folio mercantil electrónico número 37737*1, denominada **OPERADORA BESTEL, S.A. DE C.V.**, cuyo objeto social es, entre otros, la prestación de todo tipo de servicios públicos de telecomunicaciones al amparo de las concesiones y/o autorizaciones de las que sea titular, otorgadas por la autoridad competente en México.

Mediante Escritura Pública número 16,970 de fecha 03 de julio de 2007, otorgada ante la fe del Licenciado Felipe Ignacio Vázquez Aldana Sauza, Titular de la Notaría Pública número 9 de la Municipalidad de Tlaquepaque, Jalisco, se hizo constar el cambio de denominación social a **"OPERBES, S.A. DE C.V.**".

**II.2** El C. Luis Alberto De La Garza Aguirre y el C. Cesar Gerónimo Jiménez Cervantes, en su carácter de representantes legales, cuentan con facultades suficientes para suscribir el presente contrato y obligar a su representada en los términos, lo cual acreditan mediante 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, hoy Ciudad de México, e inscrita en el Registro Público de Comercio de Guadalajara, Jalisco, en el folio mercantil electrónico número 37737, mismo que bajo protesta de decir verdad manifiestan que no les han sido limitado ni revocado en forma alguna.

**II.3** 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.4** 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.

Asimismo, manifiesta que ni él ni ninguno de los socios o accionistas desempeñan un empleo, cargo o comisión en el servicio público, ni se encuentran inhabilitados para ello, o en su caso que, a pesar de desempeñarlo, con la formalización del presente contrato no se actualiza un conflicto de interés, en términos del artículo 49, fracción IX de la Ley General de Responsabilidades Administrativas.

Dirección Jurídica
Unidad de Asuntos Jurídicos
de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se pronuncia sobre la suficiencia presupuestal, viabilidad técnica, económicas y las demás circunstancias que determinan procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III del Reglamento Interior del Instituto Mexicano del Seguro Social, con relación al artículo 11 fracción I del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, Acuerdos, Convenios, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Jurídicos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número 80/DJ/CLC/0000/2020

GOBIERNO DE MÉXICO | IMSS



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

**II.5** Bajo protesta de decir verdad, declara que conoce y se obliga a cumplir con el Convenio 138 de la Organización Internacional del Trabajo en materia de erradicación del Trabajo Infantil, del artículo 123 Constitucional, apartado A) en todas sus fracciones y de la Ley Federal del Trabajo en su artículo 22, manifestando que ni en sus registros, ni en su nómina tiene empleados menores de quince años y que en caso de llegar a tener a menores de dieciocho años que se encuentren dentro de los supuestos de edad permitida para laborar le serán respetados todos los derechos que se establecen en el marco normativo transcrito.

**II.6** Cuenta con su Registro Federal de Contribuyentes **OPE070326DNA.**

**II.7** Cuenta con el documento vigente expedido por el Servicio de Administración Tributaria (SAT), de opinión de cumplimiento de obligaciones fiscales en sentido positivo, de conformidad con el artículo 32 D del Código Fiscal de la Federación, así como a lo dispuesto por las Reglas 2.1.29 y 2.1.37 de la Resolución Miscelánea Fiscal para 2022, publicada el 27 de diciembre de 2021 en el Diario Oficial de la Federación, del cual presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

**II.8** Sus trabajadores se encuentran inscritos en el régimen obligatorio del Seguro Social, y al corriente en el pago de las cuotas obrero patronales a que haya lugar, conforme a lo dispuesto en la Ley del Seguro Social, cuyas constancias correspondientes debidamente emitidas por **"EL INSTITUTO"** se verificaron para efectos de la suscripción del presente instrumento jurídico.

**II.9** Cuenta con el documento correspondiente vigente, expedido por **"EL INSTITUTO"** sobre el cumplimiento de sus obligaciones fiscales en materia de seguridad social, conforme al Acuerdo ACDO.AS2.HCT.270422/107.P.DIR dictado por el H. Consejo Técnico de **"EL INSTITUTO"** en la sesión ordinaria celebrada el 27 de abril de 2022, publicado en el Diario Oficial de la Federación el 22 de septiembre de 2022, el cual se verificó para efectos de la suscripción del presente contrato.

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

**II.10** Cuenta con el documento correspondiente vigente, expedido por el INFONAVIT en los términos del Acuerdo del H. Consejo de Administración del Instituto del Fondo Nacional de la Vivienda para los Trabajadores por el que se emiten las Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos, publicado en el Diario Oficial de la Federación el 28 de junio de 2017, del cual presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

**II.11** Señala como su domicilio para todos los efectos legales, para oír y recibir toda clase de notificaciones y documentos, el ubicado en Avenida Javier Barros Sierra número 540, Torre II, Colonia Lomas de Santa Fe, Demarcación Territorial Álvaro Obregón, Código



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

Postal 01219, Ciudad de México, teléfono: 5540002195, correo electrónico: [redacted]

**II.12** Conforme a lo previsto en los artículos 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 107 de su Reglamento, **"EL PROVEEDOR"**, en caso de auditorías, visitas o inspecciones que practique la Secretaría de la Función Pública y el Órgano Interno de Control en **"EL INSTITUTO"** y cualquier otra entidad fiscalizadora, deberá proporcionar la información relativa al presente contrato que en su momento se requiera, generada desde el procedimiento de adjudicación hasta la conclusión de la vigencia, a efecto de ser sujetos a fiscalización de los recursos de carácter federal.

**SILENT4BUSINESS, S.A. DE C.V.** (El Participante B)

**II.13** Es una persona moral legalmente constituida según consta en la Escritura Pública número 61,579 de fecha 25 de julio de 2016, pasada ante la fe del Licenciado Guillermo Oliver Bucio, Titular de la Notaría Pública número 246 de la Ciudad de México, en el protocolo de la Notaría número 212, por convenio de sociedad con su titular el Licenciado Francisco I. Hugues Vélez, e inscrita en el Registro Público de la Propiedad y de Comercio de la misma Entidad, en el folio mercantil electrónico número 561326-1, denominada **SILENT4BUSINESS, S.A. DE C.V.**, cuyo objeto social es, entre otros, la comercialización de servicios de información en el área de investigación técnica y científica, practicar toda clase de investigaciones y estudios sobre la potencialidad y tendencias de mercado, rendir toda clase de asesoría y servicios técnicos y especializados en el análisis, elaboración, mantenimiento, actualización y procedimiento electrónico de datos y estadísticas médicas o científicas y prestar servicios de consultoría en promoción de ventas, organización de seminarios y cursos en mercadotecnia para toda clase de sociedades o empresas de sector público o privado; la compraventa, importación, exportación, comercialización, intermediación y comisión de todo tipo de equipo de informática incluyendo el "software" y "hardware" así como todo tipo de paquetes relacionados con la informática.

**II.14** El C. Gerardo Garibay Aymes, en su carácter de representante legal, cuenta con facultades suficientes para suscribir el presente contrato y obligar a su representada en los términos, lo cual acredita mediante la Escritura Pública número 997 de fecha 08 de marzo de 2021, pasada ante la fe del Licenciado Gustavo Fernández Sauri, Titular de la Notaría Pública número 184 del Estado de México, mismo que bajo protesta de decir verdad manifiesta que no le han sido limitado ni revocado en forma alguna.

**II.15** 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.16** 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.

Dirección Jurídica
Unidad de Asuntos Jurídicos
de Atención a Órganos Fiscalizadores
Coordinación de Legalización y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se revisan las cuestiones técnicas, financieras, de calidad, oportunidad, económicas y las demás circunstancias que determinen procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en el artículo 19 fracción I del Reglamento de la Dirección Jurídica. Convenios, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número: 5GCLCONSU-2021/2007

GOBIERNO DE MÉXICO

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: CORREO ELECTRÓNICO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN I Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016

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.

Asimismo, manifiesta que ni él ni ninguno de los socios o accionistas desempeñan un empleo, cargo o comisión en el servicio público, ni se encuentran inhabilitados para ello, o en su caso que, a pesar de desempeñarlo, con la formalización del presente contrato no se actualiza un conflicto de interés, en términos del artículo 49, fracción IX de la Ley General de Responsabilidades Administrativas.

**II.17** Bajo protesta de decir verdad, declara que conoce y se obliga a cumplir con el Convenio 138 de la Organización Internacional del Trabajo en materia de erradicación del Trabajo Infantil, del artículo 123 Constitucional, apartado A) en todas sus fracciones y de la Ley Federal del Trabajo en su artículo 22, manifestando que ni en sus registros, ni en su nómina tiene empleados menores de quince años y que en caso de llegar a tener a menores de dieciocho años que se encuentren dentro de los supuestos de edad permitida para laborar le serán respetados todos los derechos que se establecen en el marco normativo transcrito.

**II.18** Cuenta con su Registro Federal de Contribuyentes **SIL160727HV7.**

**II.19** Cuenta con el documento vigente expedido por el Servicio de Administración Tributaria (SAT), de opinión de cumplimiento de obligaciones fiscales en sentido positivo, de conformidad con el artículo 32 D del Código Fiscal de la Federación, así como a lo dispuesto por las Reglas 2.1.29 y 2.1.37 de la Resolución Miscelánea Fiscal para 2022, publicada el 27 de diciembre de 2021 en el Diario Oficial de la Federación, del cual presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

**II.20** Sus trabajadores se encuentran inscritos en el régimen obligatorio del Seguro Social, y al corriente en el pago de las cuotas obrero patronales a que haya lugar, conforme a lo dispuesto en la Ley del Seguro Social, cuyas constancias correspondientes debidamente emitidas por **"EL INSTITUTO"** se verificaron para efectos de la suscripción del presente instrumento jurídico.

**II.21** Cuenta con el documento correspondiente vigente, expedido por **"EL INSTITUTO"** sobre el cumplimiento de sus obligaciones fiscales en materia de seguridad social, conforme al Acuerdo ACDO.AS2.HCT.270422/107.P.DIR dictado por el H. Consejo Técnico de **"EL INSTITUTO"** en la sesión ordinaria celebrada el 27 de abril de 2022, publicado en el Diario Oficial de la Federación el 22 de septiembre de 2022, el cual se verificó para efectos de la suscripción del presente contrato.

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

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se responsabiliza sobre la veracidad, suficiencia y validez de la información económicas y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con base en el artículo Primero Fracción II del Acuerdo por el que se delegan facultades en los titulares de la Dirección de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número: DO/DDJC/AOF/23/007

GOBIERNO DE MÉXICO

**II.22** Cuenta con el documento correspondiente vigente, expedido por el INFONAVIT en los términos del Acuerdo del H. Consejo de Administración del Instituto del Fondo Nacional de la Vivienda para los Trabajadores por el que se emiten las Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos, publicado en el Diario Oficial de la Federación el 28 de junio de 2017, del cual presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

**II.23** Señala como su domicilio para todos los efectos legales, para oír y recibir toda clase de notificaciones y documentos, el ubicado en Avenida Insurgentes Sur número 2453, Piso 4, Colonia Tizapán San Ángel, Demarcación Territorial Álvaro Obregón, Código Postal 01090, Ciudad de México, teléfono: 55 7328 3000, correo electrónico: contacto@silent4business.com

**II.24** Conforme a lo previsto en los artículos 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 107 de su Reglamento, **"EL PROVEEDOR"**, en caso de auditorías, visitas o inspecciones que practique la Secretaría de la Función Pública y el Órgano Interno de Control en **"EL INSTITUTO"** y cualquier otra entidad fiscalizadora, deberá proporcionar la información relativa al presente contrato que en su momento se requiera, generada desde el procedimiento de adjudicación hasta la conclusión de la vigencia, a efecto de ser sujetos a fiscalización de los recursos de carácter federal.

**BUFETE EMPRESARIAL GTI, S.A. DE C.V.** (El Participante C)

**II.25** Es una persona moral legalmente constituida según consta en la Escritura Pública número 53,929 de fecha 27 de noviembre de 2014, pasada ante la fe del Licenciado Pedro Cortina Latapi, Titular de la Notaría Pública número 226 del Distrito Federal, hoy Ciudad de México, e inscrita en el Registro Público de la Propiedad y de Comercio de la misma Entidad, en el folio mercantil electrónico número 527176-1, denominada **BUFETE EMPRESARIAL GTI, S.A. DE C.V.**, cuyo objeto social es, entre otros, la compra, venta, renta, distribución, importación, exportación, almacenamiento, maquila y fabricación de equipo electrónico de comunicación, equipo y accesorios de tecnologías de la información, seguridad de redes informáticas, administración de base de datos, fabricación de equipo de radio, comunicación, refacciones y partes, componentes, alarmas electrónicas, de video, circuitos cerrados de televisión, radio y televisión comercial, equipo contra incendios, ropa y muebles metálicos y de madera así como el diseño de redes de radiocomunicación, computo, alarmas contra incendios y circuitos de televisión y radio.

**II.26** El C. Juan Luis Pineda González, en su carácter de representante legal, cuenta con facultades suficientes para suscribir el presente contrato y obligar a su representada en los términos, lo cual acredita mediante la Escritura Pública número 71,945 de fecha 11 de junio de 2019, pasada ante la fe del Licenciado Miguel Ángel Beltrán Lara, Titular de la Notaría Pública número 169 de la Ciudad de México, mismo que bajo protesta de decir verdad manifiesta que no le han sido limitado ni revocado en forma alguna.

Dirección Jurídica
Unidad de Asuntos Jurídicos, Gobierno y de Atención a Órganos Fiscalizadores
Coordinación de Legalización y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se manifiesta sobre la procedencia técnica, económica, financiera, jurídica, económicas y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con base en el artículo Segundo, fracción I, inciso a) del Acuerdo que delega facultades a favor de las personas titulares de la Coordinación de Legalización y Consulta, de la Unidad de Asuntos Jurídicos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número: 0428/DOC/CLC/2019/07

GOBIERNO DE MÉXICO



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

**II.27** 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.28** 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.

Asimismo, manifiesta que ni él ni ninguno de los socios o accionistas desempeñan un empleo, cargo o comisión en el servicio público, ni se encuentran inhabilitados para ello, o en su caso que, a pesar de desempeñarlo, con la formalización del presente contrato no se actualiza un conflicto de interés, en términos del artículo 49, fracción IX de la Ley General de Responsabilidades Administrativas.

**II.29** Bajo protesta de decir verdad, declara que conoce y se obliga a cumplir con el Convenio 138 de la Organización Internacional del Trabajo en materia de erradicación del Trabajo Infantil, del artículo 123 Constitucional, apartado A) en todas sus fracciones y de la Ley Federal del Trabajo en su artículo 22, manifestando que ni en sus registros, ni en su nómina tiene empleados menores de quince años y que en caso de llegar a tener a menores de dieciocho años que se encuentren dentro de los supuestos de edad permitida para laborar le serán respetados todos los derechos que se establecen en el marco normativo transcrito.

**II.30** Cuenta con su Registro Federal de Contribuyentes **BEG141128JD5.**

**II.31** Cuenta con el documento vigente expedido por el Servicio de Administración Tributaria (SAT), de opinión de cumplimiento de obligaciones fiscales en sentido positivo, de conformidad con el artículo 32 D del Código Fiscal de la Federación, así como a lo dispuesto por las Reglas 2.1.29 y 2.1.37 de la Resolución Miscelánea Fiscal para 2022, publicada el 27 de diciembre de 2021 en el Diario Oficial de la Federación, del cual presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

**II.32** Sus trabajadores se encuentran inscritos en el régimen obligatorio del Seguro Social, y al corriente en el pago de las cuotas obrero patronales a que haya lugar, conforme a lo dispuesto en la Ley del Seguro Social, cuyas constancias correspondientes debidamente emitidas por **"EL INSTITUTO"** se verificaron para efectos de la suscripción del presente instrumento jurídico.

**II.33** Cuenta con el documento correspondiente vigente, expedido por **"EL INSTITUTO"** sobre el cumplimiento de sus obligaciones fiscales en materia de seguridad social, conforme al Acuerdo ACDO.AS2.HCT.270422/107.P.DIR dictado por el H. Consejo Técnico de **"EL INSTITUTO"** en la sesión ordinaria celebrada el 27 de abril de 2022, publicado en el

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado realizada, así como de la viabilidad de los aspectos técnicos, económicos y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en los artículos 19 fracción VI y 20 fracción VI del Reglamento de la Comisión, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número: DGDSUCAJO/0310/2021

GOBIERNO DE MÉXICO | IMSS

Diario Oficial de la Federación el 22 de septiembre de 2022, el cual se verificó para efectos de la suscripción del presente contrato.

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

**II.34** Cuenta con el documento correspondiente vigente, expedido por el INFONAVIT en los términos del Acuerdo del H. Consejo de Administración del Instituto del Fondo Nacional de la Vivienda para los Trabajadores por el que se emiten las Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos, publicado en el Diario Oficial de la Federación el 28 de junio de 2017, del cual presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

**II.35** Señala como su domicilio para todos los efectos legales, para oír y recibir toda clase de notificaciones y documentos, el ubicado en calle Pensylvania número 127, Colonia Nápoles, Demarcación Territorial Benito Juárez, Código Postal 03810, Ciudad de México, teléfono: 55 1764 7125, correo electrónico: [redacted]

**II.36** Conforme a lo previsto en los artículos 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 107 de su Reglamento, **"EL PROVEEDOR"**, en caso de auditorías, visitas o inspecciones que practique la Secretaría de la Función Pública y el Órgano Interno de Control en **"EL INSTITUTO"** y cualquier otra entidad fiscalizadora, deberá proporcionar la información relativa al presente contrato que en su momento se requiera, generada desde el procedimiento de adjudicación hasta la conclusión de la vigencia, a efecto de ser sujetos a fiscalización de los recursos de carácter federal.

**III.- "EL PROVEEDOR"** declara, conjuntamente, que:

**III.1.-** Han celebrado un convenio de participación conjunta, cuyas obligaciones deberán cumplirse en términos del mismo, el cual se integra al presente instrumento jurídico como **Anexo 6 (seis).**

**III.2.-** Conocen el contenido y los requisitos que establece la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento, la Convocatoria y sus Anexos.

Hecho el antecedente y declaraciones anteriores, **"LAS PARTES"** convienen otorgar el presente contrato, de conformidad con las siguientes:

**C L Á U S U L A S**

**PRIMERA. OBJETO DEL CONTRATO.**

**SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: CORREO ELECTRÓNICO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN I Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016**



Dirección Jurídica
Unidad de Asuntos Contenciosos
de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se revisan cuestiones técnicas, económicas, financieras o de cualquier índole económicos y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

GOBIERNO DE MÉXICO | IMSS

Los aspectos jurídicos del presente instrumento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en los artículos 2 fracción I, 4 fracción I, 5 fracción I, 6 fracción I, 7 fracción I, 8 fracción I, 9 fracción I, 10 fracción I, 11 fracción I, 12 fracción I, 13 fracción I, 14 fracción I, 15 fracción I, 16 fracción I,

**"EL PROVEEDOR"** acepta y se obliga a proporcionar a **"EL INSTITUTO"** los "Servicios Administrados de Seguridad Informática (SASI) 2022-2024" (Partida 1), al amparo del procedimiento de contratación señalado en el antecedente de este instrumento jurídico.

Los **Anexos** que forman parte integrante del presente contrato, se enuncian a continuación:

| | |
|---|---|
| **Anexo 1 (uno)** | "Dictamen de Disponibilidad Presupuestal Previo y Acuerdo del H. Consejo Técnico". |
| **Anexo 2 (dos)** | "Anexo Técnico y Términos y Condiciones" |
| **Anexo 3 (tres)** | "Propuesta Técnica y Económica de **"EL PROVEEDOR"** y Acta de Fallo" |
| **Anexo 4 (cuatro)** | "Documento de Designación de Administrador del Contrato" |
| **Anexo 5 (cinco)** | "Junta de Aclaraciones, la cual se encuentra disponible para su consulta en CompraNet" |
| **Anexo 6 (seis)** | "Convenio de Participación Conjunta" |

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se asume responsabilidad alguna por la veracidad de la información técnica, económicas y las demás circunstancias que determinaron precedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en los artículos 1, 2 fracción I, 3 fracción II, 4 fracción II, 5 fracción II, 6 fracción II, 7 fracción II, 8 fracción II, 9 fracción II, 10 fracción II, 11 fracción II, 12 fracción II, 13 fracción II, 14 fracción II, 15 fracción II, 16 fracción II, 17 fracción II, 18 fracción II, 19 fracción II, 20 fracción II, 21 fracción II, 22 fracción II, 23 fracción II, 24 fracción II, 25 fracción II, 26 fracción II, 27 fracción II, 28 fracción II, 29 fracción II, 30 fracción II, 31 fracción II, 32 fracción II, 33 fracción II, 34 fracción II, 35 fracción II, 36 fracción II, 37 fracción II, 38 fracción II, 39 fracción II, 40 fracción II, 41 fracción II, 42 fracción II, 43 fracción II, 44 fracción II, 45 fracción II, 46 fracción II, 47 fracción II, 48 fracción II, 49 fracción II, 50 fracción II, 51 fracción II, 52 fracción II, 53 fracción II, 54 fracción II, 55 fracción II, 56 fracción II, 57 fracción II, 58 fracción II, 59 fracción II, 60 fracción II, 61 fracción II, 62 fracción II, 63 fracción II, 64 fracción II, 65 fracción II, 66 fracción II, 67 fracción II, 68 fracción II, 69 fracción II, 70 fracción II, 71 fracción II, 72 fracción II, 73 fracción II, 74 fracción II, 75 fracción II, 76 fracción II, 77 fracción II, 78 fracción II, 79 fracción II, 80 fracción II, 81 fracción II, 82 fracción II, 83 fracción II, 84 fracción II, 85 fracción II, 86 fracción II, 87 fracción II, 88 fracción II, 89 fracción II, 90 fracción II, 91 fracción II, 92 fracción II, 93 fracción II, 94 fracción II, 95 fracción II, 96 fracción II, 97 fracción II, 98 fracción II, 99 fracción II, 100 fracción II, 101 fracción II, 102 fracción II, 103 fracción II, 104 fracción II, 105 fracción II, 106 fracción II, 107 fracción II, 108 fracción II, 109 fracción II, 110 fracción II, 111 fracción II, 112 fracción II, 113 fracción II, 114 fracción II, 115 fracción II, 116 fracción II, 117 fracción II, 118 fracción II, 119 fracción II, 120 fracción II, 121 fracción II, 122 fracción II, 123 fracción II, 124 fracción II, 125 fracción II, 126 fracción II, 127 fracción II, 128 fracción II, 129 fracción II, 130 fracción II, 131 fracción II, 132 fracción II, 133 fracción II, 134 fracción II, 135 fracción II, 136 fracción II, 137 fracción II, 138 fracción II, 139 fracción II, 140 fracción II, 141 fracción II, 142 fracción II, 143 fracción II, 144 fracción II, 145 fracción II, 146 fracción II, 147 fracción II, 148 fracción II, 149 fracción II, 150 fracción II, 151 fracción II, 152 fracción II, 153 fracción II, 154 fracción II, 155 fracción II, 156 fracción II, 157 fracción II, 158 fracción II, 159 fracción II, 160 fracción II, 161 fracción II, 162 fracción II, 163 fracción II, 164 fracción II, 165 fracción II, 166 fracción II, 167 fracción II, 168 fracción II, 169 fracción II, 170 fracción II, 171 fracción II, 172 fracción II, 173 fracción II, 174 fracción II, 175 fracción II, 176 fracción II, 177 fracción II, 178 fracción II, 179 fracción II, 180 fracción II, 181 fracción II, 182 fracción II, 183 fracción II, 184 fracción II, 185 fracción II, 186 fracción II, 187 fracción II, 188 fracción II, 189 fracción II, 190 fracción II, 191 fracción II, 192 fracción II, 193 fracción II, 194 fracción II, 195 fracción II, 196 fracción II, 197 fracción II, 198 fracción II, 199 fracción II, 200 fracción II, 201 fracción II, 202 fracción II, 203 fracción II, 204 fracción II, 205 fracción II, 206 fracción II, 207 fracción II, 208 fracción II, 209 fracción II, 210 fracción II, 211 fracción II, 212 fracción II, 213 fracción II, 214 fracción II, 215 fracción II, 216 fracción II, 217 fracción II, 218 fracción II, 219 fracción II, 220 fracción II, 221 fracción II, 222 fracción II, 223 fracción II, 224 fracción II, 225 fracción II, 226 fracción II, 227 fracción II, 228 fracción II, 229 fracción II, 230 fracción II, 231 fracción II, 232 fracción II, 233 fracción II, 234 fracción II, 235 fracción II, 236 fracción II, 237 fracción II, 238 fracción II, 239 fracción II, 240 fracción II, 241 fracción II, 242 fracción II, 243 fracción II, 244 fracción II, 245 fracción II, 246 fracción II, 247 fracción II, 248 fracción II, 249 fracción II, 250 fracción II, 251 fracción II, 252 fracción II, 253 fracción II, 254 fracción II, 255 fracción II, 256 fracción II, 257 fracción II, 258 fracción II, 259 fracción II, 260 fracción II, 261 fracción II, 262 fracción II, 263 fracción II, 264 fracción II, 265 fracción II, 266 fracción II, 267 fracción II, 268 fracción II, 269 fracción II, 270 fracción II, 271 fracción II, 272 fracción II, 273 fracción II, 274 fracción II, 275 fracción II, 276 fracción II, 277 fracción II, 278 fracción II, 279 fracción II, 280 fracción II, 281 fracción II, 282 fracción II, 283 fracción II, 284 fracción II, 285 fracción II, 286 fracción II, 287 fracción II, 288 fracción II, 289 fracción II, 290 fracción II, 291 fracción II, 292 fracción II, 293 fracción II, 294 fracción II, 295 fracción II, 296 fracción II, 297 fracción II, 298 fracción II, 299 fracción II, 300 fracción II, 301 fracción II, 302 fracción II, 303 fracción II, 304 fracción II, 305 fracción II, 306 fracción II, 307 fracción II, 308 fracción II, 309 fracción II, 310 fracción II, 311 fracción II, 312 fracción II, 313 fracción II, 314 fracción II, 315 fracción II, 316 fracción II, 317 fracción II, 318 fracción II, 319 fracción II, 320 fracción II, 321 fracción II, 322 fracción II, 323 fracción II, 324 fracción II, 325 fracción II, 326 fracción II, 327 fracción II, 328 fracción II, 329 fracción II, 330 fracción II, 331 fracción II, 332 fracción II, 333 fracción II, 334 fracción II, 335 fracción II, 336 fracción II, 337 fracción II, 338 fracción II, 339 fracción II, 340 fracción II, 341 fracción II, 342 fracción II, 343 fracción II, 344 fracción II, 345 fracción II, 346 fracción II, 347 fracción II, 348 fracción II, 349 fracción II, 350 fracción II, 351 fracción II, 352 fracción II, 353 fracción II, 354 fracción II, 355 fracción II, 356 fracción II, 357 fracción II, 358 fracción II, 359 fracción II, 360 fracción II, 361 fracción II, 362 fracción II, 363 fracción II, 364 fracción II, 365 fracción II, 366 fracción II, 367 fracción II, 368 fracción II, 369 fracción II, 370 fracción II, 371 fracción II, 372 fracción II, 373 fracción II, 374 fracción II, 375 fracción II, 376 fracción II, 377 fracción II, 378 fracción II, 379 fracción II, 380 fracción II, 381 fracción II, 382 fracción II, 383 fracción II, 384 fracción II, 385 fracción II, 386 fracción II, 387 fracción II, 388 fracción II, 389 fracción II, 390 fracción II, 391 fracción II, 392 fracción II, 393 fracción II, 394 fracción II, 395 fracción II, 396 fracción II, 397 fracción II, 398 fracción II, 399 fracción II, 400 fracción II, 401 fracción II, 402 fracción II, 403 fracción II, 404 fracción II, 405 fracción II, 406 fracción II, 407 fracción II, 408 fracción II, 409 fracción II, 410 fracción II, 411 fracción II, 412 fracción II, 413 fracción II, 414 fracción II, 415 fracción II, 416 fracción II, 417 fracción II, 418 fracción II, 419 fracción II, 420 fracción II, 421 fracción II, 422 fracción II, 423 fracción II, 424 fracción II, 425 fracción II, 426 fracción II, 427 fracción II, 428 fracción II, 429 fracción II, 430 fracción II, 431 fracción II, 432 fracción II, 433 fracción II, 434 fracción II, 435 fracción II, 436 fracción II, 437 fracción II, 438 fracción II, 439 fracción II, 440 fracción II, 441 fracción II, 442 fracción II, 443 fracción II, 444 fracción II, 445 fracción II, 446 fracción II, 447 fracción II, 448 fracción II, 449 fracción II, 450 fracción II, 451 fracción II, 452 fracción II, 453 fracción II, 454 fracción II, 455 fracción II, 456 fracción II, 457 fracción II, 458 fracción II, 459 fracción II, 460 fracción II, 461 fracción II, 462 fracción II, 463 fracción II, 464 fracción II, 465 fracción II, 466 fracción II, 467 fracción II, 468 fracción II, 469 fracción II, 470 fracción II, 471 fracción II, 472 fracción II, 473 fracción II, 474 fracción II, 475 fracción II, 476 fracción II, 477 fracción II, 478 fracción II, 479 fracción II, 480 fracción II, 481 fracción II, 482 fracción II, 483 fracción II, 484 fracción II, 485 fracción II, 486 fracción II, 487 fracción II, 488 fracción II, 489 fracción II, 490 fracción II, 491 fracción II, 492 fracción II, 493 fracción II, 494 fracción II, 495 fracción II, 496 fracción II, 497 fracción II, 498 fracción II, 499 fracción II, 500 fracción II, 501 fracción II, 502 fracción II, 503 fracción II, 504 fracción II, 505 fracción II, 506 fracción II, 507 fracción II, 508 fracción II, 509 fracción II, 510 fracción II, 511 fracción II, 512 fracción II, 513 fracción II, 514 fracción II, 515 fracción II, 516 fracción II, 517 fracción II, 518 fracción II, 519 fracción II, 520 fracción II, 521 fracción II, 522 fracción II, 523 fracción II, 524 fracción II, 525 fracción II, 526 fracción II, 527 fracción II, 528 fracción II, 529 fracción II, 530 fracción II, 531 fracción II, 532 fracción II, 533 fracción II, 534 fracción II, 535 fracción II, 536 fracción II, 537 fracción II, 538 fracción II, 539 fracción II, 540 fracción II, 541 fracción II, 542 fracción II, 543 fracción II, 544 fracción II, 545 fracción II, 546 fracción II, 547 fracción II, 548 fracción II, 549 fracción II, 550 fracción II, 551 fracción II, 552 fracción II, 553 fracción II, 554 fracción II, 555 fracción II, 556 fracción II, 557 fracción II, 558 fracción II, 559 fracción II, 560 fracción II, 561 fracción II, 562 fracción II, 563 fracción II, 564 fracción II, 565 fracción II, 566 fracción II, 567 fracción II, 568 fracción II, 569 fracción II, 570 fracción II, 571 fracción II, 572 fracción II, 573 fracción II, 574 fracción II, 575 fracción II, 576 fracción II, 577 fracción II, 578 fracción II, 579 fracción II, 580 fracción II, 581 fracción II, 582 fracción II, 583 fracción II, 584 fracción II, 585 fracción II, 586 fracción II, 587 fracción II, 588 fracción II, 589 fracción II, 590 fracción II, 591 fracción II, 592 fracción II, 593 fracción II, 594 fracción II, 595 fracción II, 596 fracción II, 597 fracción II, 598 fracción II, 599 fracción II, 600 fracción II, 601 fracción II, 602 fracción II, 603 fracción II, 604 fracción II, 605 fracción II, 606 fracción II, 607 fracción II, 608 fracción II, 609 fracción II, 610 fracción II, 611 fracción II, 612 fracción II, 613 fracción II, 614 fracción II, 615 fracción II, 616 fracción II, 617 fracción II, 618 fracción II, 619 fracción II, 620 fracción II, 621 fracción II, 622 fracción II, 623 fracción II, 624 fracción II, 625 fracción II, 626 fracción II, 627 fracción II, 628 fracción II, 629 fracción II, 630 fracción II, 631 fracción II, 632 fracción II, 633 fracción II, 634 fracción II, 635 fracción II, 636 fracción II, 637 fracción II, 638 fracción II, 639 fracción II, 640 fracción II, 641 fracción II, 642 fracción II, 643 fracción II, 644 fracción II, 645 fracción II, 646 fracción II, 647 fracción II, 648 fracción II, 649 fracción II, 650 fracción II, 651 fracción II, 652 fracción II, 653 fracción II, 654 fracción II, 655 fracción II, 656 fracción II, 657 fracción II, 658 fracción II, 659 fracción II, 660 fracción II, 661 fracción II, 662 fracción II, 663 fracción II, 664 fracción II, 665 fracción II, 666 fracción II, 667 fracción II, 668 fracción II, 669 fracción II, 670 fracción II, 671 fracción II, 672 fracción II, 673 fracción II, 674 fracción II, 675 fracción II, 676 fracción II, 677 fracción II, 678 fracción II, 679 fracción II, 680 fracción II, 681 fracción II, 682 fracción II, 683 fracción II, 684 fracción II, 685 fracción II, 686 fracción II, 687 fracción II, 688 fracción II, 689 fracción II, 690 fracción II, 691 fracción II, 692 fracción II, 693 fracción II, 694 fracción II, 695 fracción II, 696 fracción II, 697 fracción II, 698 fracción II, 699 fracción II, 700 fracción II, 701 fracción II, 702 fracción II, 703 fracción II, 704 fracción II, 705 fracción II, 706 fracción II, 707 fracción II, 708 fracción II, 709 fracción II, 710 fracción II, 711 fracción II, 712 fracción II, 713 fracción II, 714 fracción II, 715 fracción II, 716 fracción II, 717 fracción II, 718 fracción II, 719 fracción II, 720 fracción II, 721 fracción II, 722 fracción II, 723 fracción II, 724 fracción II, 725 fracción II, 726 fracción II, 727 fracción II, 728 fracción II, 729 fracción II, 730 fracción II, 731 fracción II, 732 fracción II, 733 fracción II, 734 fracción II, 735 fracción II, 736 fracción II, 737 fracción II, 738 fracción II, 739 fracción II, 740 fracción II, 741 fracción II, 742 fracción II, 743 fracción II, 744 fracción II, 745 fracción II, 746 fracción II, 747 fracción II, 748 fracción II, 749 fracción II, 750 fracción II, 751 fracción II, 752 fracción II, 753 fracción II, 754 fracción II, 755 fracción II, 756 fracción II, 757 fracción II, 758 fracción II, 759 fracción II, 760 fracción II, 761 fracción II, 762 fracción II, 763 fracción II, 764 fracción II, 765 fracción II, 766 fracción II, 767 fracción II, 768 fracción II, 769 fracción II, 770 fracción II, 771 fracción II, 772 fracción II, 773 fracción II, 774 fracción II, 775 fracción II, 776 fracción II, 777 fracción II, 778 fracción II, 779 fracción II, 780 fracción II, 781 fracción II, 782 fracción II, 783 fracción II, 784 fracción II, 785 fracción II, 786 fracción II, 787 fracción II, 788 fracción II, 789 fracción II, 790 fracción II, 791 fracción II, 792 fracción II, 793 fracción II, 794 fracción II, 795 fracción II, 796 fracción II, 797 fracción II, 798 fracción II, 799 fracción II, 800 fracción II, 801 fracción II, 802 fracción II, 803 fracción II, 804 fracción II, 805 fracción II, 806 fracción II, 807 fracción II, 808 fracción II, 809 fracción II, 810 fracción II, 811 fracción II, 812 fracción II, 813 fracción II, 814 fracción II, 815 fracción II, 816 fracción II, 817 fracción II, 818 fracción II, 819 fracción II, 820 fracción II, 821 fracción II, 822 fracción II, 823 fracción II, 824 fracción II, 825 fracción II, 826 fracción II, 827 fracción II, 828 fracción II, 829 fracción II, 830 fracción II, 831 fracción II, 832 fracción II, 833 fracción II, 834 fracción II, 835 fracción II, 836 fracción II, 837 fracción II, 838 fracción II, 839 fracción II, 840 fracción II, 841 fracción II, 842 fracción II, 843 fracción II, 844 fracción II, 845 fracción II, 846 fracción II, 847 fracción II, 848 fracción II, 849 fracción II, 850 fracción II, 851 fracción II, 852 fracción II, 853 fracción II, 854 fracción II, 855 fracción II, 856 fracción II, 857 fracción II, 858 fracción II, 859 fracción II, 860 fracción II, 861 fracción II, 862 fracción II, 863 fracción II, 864 fracción II, 865 fracción II, 866 fracción II, 867 fracción II, 868 fracción II, 869 fracción II, 870 fracción II, 871 fracción II, 872 fracción II, 873 fracción II, 874 fracción II, 875 fracción II, 876 fracción II, 877 fracción II, 878 fracción II, 879 fracción II, 880 fracción II, 881 fracción II, 882 fracción II, 883 fracción II, 884 fracción II, 885 fracción II, 886 fracción II, 887 fracción II, 888 fracción II, 889 fracción II, 890 fracción II, 891 fracción II, 892 fracción II, 893 fracción II, 894 fracción II, 895 fracción II, 896 fracción II, 897 fracción II, 898 fracción II, 899 fracción II, 900 fracción II, 901 fracción II, 902 fracción II, 903 fracción II, 904 fracción II, 905 fracción II, 906 fracción II, 907 fracción II, 908 fracción II, 909 fracción II, 910 fracción II, 911 fracción II, 912 fracción II, 913 fracción II, 914 fracción II, 915 fracción II, 916 fracción II, 917 fracción II, 918 fracción II, 919 fracción II, 920 fracción II, 921 fracción II, 922 fracción II, 923 fracción II, 924 fracción II, 925 fracción II, 926 fracción II, 927 fracción II, 928 fracción II, 929 fracción II, 930 fracción II, 931 fracción II, 932 fracción II, 933 fracción II, 934 fracción II, 935 fracción II, 936 fracción II, 937 fracción II, 938 fracción II, 939 fracción II, 940 fracción II, 941 fracción II, 942 fracción II, 943 fracción II, 944 fracción II, 945 fracción II, 946 fracción II, 947 fracción II, 948 fracción II, 949 fracción II, 950 fracción II, 951 fracción II, 952 fracción II, 953 fracción II, 954 fracción II, 955 fracción II, 956 fracción II, 957 fracción II, 958 fracción II, 959 fracción II, 960 fracción II, 961 fracción II, 962 fracción II, 963 fracción II, 964 fracción II, 965 fracción II, 966 fracción II, 967 fracción II, 968 fracción II, 969 fracción II, 970 fracción II, 971 fracción II, 972 fracción II, 973 fracción II, 974 fracción II, 975 fracción II, 976 fracción II, 977 fracción II, 978 fracción II, 979 fracción II, 980 fracción II, 981 fracción II, 982 fracción II, 983 fracción II, 984 fracción II, 985 fracción II, 986 fracción II, 987 fracción II, 988 fracción II, 989 fracción II, 990 fracción II, 991 fracción II, 992 fracción II, 993 fracción II, 994 fracción II, 995 fracción II, 996 fracción II, 997 fracción II, 998 fracción II, 999 fracción II, 1000 fracción II.

GOBIERNO DE MÉXICO | IMSS

Este documento fue firmado electrónicamente con FIEL del SAT, con validez jurídica conforme a los artículos 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000 fracción II.

**SEGUNDA. DE LOS MONTOS Y PRECIOS.**

El monto mínimo del presente contrato es por la cantidad de **$138,499,360.00 (CIENTO TREINTA Y OCHO MILLONES CUATROCIENTOS NOVENTA Y NUEVE MIL TRESCIENTOS SESENTA PESOS 00/100 M.N.),** incluyendo el Impuesto al Valor Agregado (I.V.A.), y el monto máximo del mismo es por la cantidad de **$346,248,400.00 (TRESCIENTOS CUARENTA Y SEIS MILLONES DOSCIENTOS CUARENTA Y OCHO MIL CUATROCIENTOS PESOS 00/100 M.N.),** incluyendo el Impuesto al Valor Agregado (I.V.A.), los precios unitarios del presente contrato son por las cantidades señaladas en la propuesta económica de **"EL PROVEEDOR"**, que se agrega en el **Anexo 3 (tres)**.

Los montos mínimos y máximos por cada ejercicio fiscal son los siguientes:

| PARTIDA 1 | | | | |
|---|---|---|---|---|
| **MONTOS** | **AÑO** | | | **TOTAL** |
| | **2022** | **2023** | **2024** | |
| IMPORTE MÁXIMO INCLUYENDO IVA | $43,281,050.00 | $173,124,200.00 | $129,843,150.00 | **$346,248,400.00** |
| IMPORTE MÍNIMO INCLUYENDO IVA | $17,312,420.00 | $69,249,680.00 | $51,937,260.00 | **$138,499,360.00** |

El monto y distribución de los ejercicios fiscales 2023 y 2024 estará sujeto para fines de ejecución y pago, a la disponibilidad presupuestaria con que cuente **"EL INSTITUTO"**, en el ejercicio fiscal de que se trate, conforme al Presupuesto de Egresos de la Federación que apruebe la H. Cámara de Diputados del Congreso de la Unión, sin responsabilidad alguna para **"EL INSTITUTO"**.

Los precios unitarios son considerados fijos y en moneda nacional (pesos mexicanos) hasta que concluya la relación contractual que se formaliza, incluyendo **"EL PROVEEDOR"** todos los

conceptos y costos involucrados en la prestación de los "Servicios Administrados de Seguridad Informática (SASI) 2022-2024" (Partida 1), por lo que **"EL PROVEEDOR"** no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.

**TERCERA. FORMA Y LUGAR DE PAGO.**

Se efectuarán pagos progresivos a **"EL PROVEEDOR"**, una vez prestados los servicios, de conformidad con lo dispuesto en el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como por lo establecido en el Anexo Técnico y los Términos y Condiciones que se agregan al presente contrato en el **Anexo 2 (dos)**.

El Comprobante Fiscal Digital por Internet (CFDI) deberá ser presentado en forma impresa.

El pago se realizará en pesos mexicanos, a mes vencido conforme a las entregas programadas, en los plazos normados por la Dirección de Finanzas, de acuerdo al "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos" sin que éstos rebasen los 20 (veinte) días naturales posteriores a aquel en que **"EL PROVEEDOR"** presente en forma impresa el CFDI, en la División de Tramite de Erogaciones, situada en calle Gobernador Tiburcio Montiel No. 15, Colonia San Miguel Chapultepec, Demarcación Territorial Miguel Hidalgo, Código Postal 11850, Ciudad de México, en días y horas hábiles, previa validación y autorización que para tal efecto realice el administrador del contrato, siempre y cuando se cuente con la suficiencia presupuestal, así como con la documentación comprobatoria que acredite la prestación del servicio señalada en el numeral 11 de los Términos y Condiciones que se agregan en el **Anexo 2 (dos)** del presente contrato y conforme a los numerales cuarto y sexto del capítulo quinto, intitulado, de los Lineamientos para promover la agilización de pago a los proveedores contenidos en el "Acuerdo por el que se emiten diversos lineamientos en materia de adquisiciones, arrendamientos y servicios y de obras públicas y servicios relacionados con las mismas", concordante con los artículos 65 y 66 del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.

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

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

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se pronuncia sobre la viabilidad técnica, económica, financiera o cualquier otra distinta a las jurídicas, ni sobre las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en los artículos 19 fracción VI y 20 fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, Convenios, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número DJ/DSC/CLC/0220/2021

GOBIERNO DE MÉXICO | IMSS

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

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

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

Para la validación de dichos comprobantes **"EL PROVEEDOR"** deberá cargar en Internet, a través del Portal de Servicios a Proveedores de la página de **"EL INSTITUTO"** archivo en formato XML. La validez de los mismos, será determinada durante la carga y únicamente los comprobantes validos serán procedentes para pago.

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

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

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

En ningún caso, se deberá autorizar el pago 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"** 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"**.

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se emite opinión alguna sobre aspectos técnicos, financieros, económicos y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en el artículo 19 fracción I, del Reglamento de Adquisiciones, Arrendamientos y Servicios, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número: 0GD03CC/0/0/2020/07

GOBIERNO DE MÉXICO

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".**

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

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

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

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

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

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

• La solicitud la realizará al administrador del presente 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.



Dirección Jurídica
Unidad de Asuntos Consultivos
de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, el resultado de la investigación de mercado correspondiente, ni el cumplimiento de los requisitos técnicos, financieros, económicos y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con relación a los artículos 2 fracción I, 3 fracción I, 4 fracción I, 5 fracción I, 6 fracción I, 7 fracción I, 8 fracción I, 9 fracción I, 10 fracción I, 11 fracción I, 12 fracción I, 13 fracción I, 14 fracción I,

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

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

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

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

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

El CFDI se deberá presentar desglosando el I.V.A., cuando aplique.

**"EL PROVEEDOR"** manifiesta su conformidad de que hasta en tanto no se cumpla con la verificación, supervisión y aceptación del servicio, no se tendrán como recibidos o aceptados por el administrador del presente contrato mencionado en la Declaración I.3.

Para efectos de trámite de pago, **"EL PROVEEDOR"** deberá ser titular de una cuenta de cheques vigente y para tal efecto proporciona la CLABE [redacted] del Banco [redacted] a nombre de "**OPERBES, S.A. DE C.V.**", en la que se efectuará la transferencia electrónica de pago.

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se pronuncia sobre aspectos técnicos, económicos y financieros, ni sobre las condiciones económicas y las demás circunstancias que determinaron precedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en el artículo 19 fracción I del Acuerdo por el que se delegan facultades a las personas titulares de la Unidad de Asuntos Consultivos, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el folio No. DG/DJ/DCO/CLC/2020/2007

GOBIERNO DE MÉXICO



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

SE CANCELAN DATOS PERSONALES DE PERSONA(S) MORALES IDENTIFICABLE(S) TALES COMO: CLABE Y NOMBRE DE BANCO, POR CONSIDERARSE INHERENTE AL PATRIMONIO DE LA PERSONA MORAL, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN III Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016

El pago del servicio proporcionado, quedará condicionado proporcionalmente al pago que **"EL PROVEEDOR"** deba efectuar por concepto de penas convencionales.

Para efectos del cobro de sus CFDI, deberá presentarse por **"EL PROVEEDOR"** que se haya establecido en el convenio de participación conjunta, el cual se agrega al presente instrumento jurídico como **Anexo 6 (seis)**, en el entendido de que **"EL INSTITUTO"** no será responsable de la manera en que hayan acordado la distribución del pago.

**CUARTA. VIGENCIA.**

El contrato comprenderá una vigencia considerada a partir del día hábil siguiente a la notificación del fallo y hasta el 30 de septiembre de 2024, sin perjuicio de su posible terminación anticipada, en los términos establecidos en su clausulado.

**QUINTA. MODIFICACIONES DEL PRESENTE CONTRATO.**

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.

**SEXTA. GARANTÍA DE CUMPLIMIENTO DEL PRESENTE CONTRATO.**

**"EL PROVEEDOR"** se obliga a entregar a más tardar dentro de los 10 (diez) días naturales posteriores a la firma de este instrumento jurídico, en términos de la fracción II del artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, una garantía de cumplimiento de todas y cada una de las obligaciones a su cargo derivadas del presente contrato, mediante fianza expedida por compañía autorizada en los términos de la Ley de Instituciones de Seguros y de Fianzas a favor del "Instituto Mexicano del Seguro Social" por un monto equivalente al 10% (diez por ciento) sobre el importe máximo que se indica en la Cláusula Segunda del presente contrato o por el 10% (diez por ciento) del monto máximo del ejercicio fiscal que corresponda, ambas en moneda nacional y sin incluir el Impuesto al Valor

Dirección Jurídica
Unidad de Atención Consultiva y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, el del resultado de la investigación de mercado correspondiente, ni se pronuncia sobre la suficiencia presupuestal, viabilidad técnica, económicas y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III del Reglamento Interior del Instituto Mexicano del Seguro Social, con motivo de la celebración del presente instrumento jurídico, así como sus Convenios, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el folio/nomenclatura: DCJ/CLC/UACAOF/2020

GOBIERNO DE MÉXICO | IMSS

Agregado (IVA), esta última será renovada para cada uno de los ejercicios fiscales y deberá presentarse a más tardar dentro de los primeros 10 (diez) días naturales del ejercicio que corresponda.

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

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

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

**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 presente Cláusula.

**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.

**SÉPTIMA. OBLIGACIONES DE "EL PROVEEDOR".**

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni tampoco sobre la viabilidad técnica, económica y financiera, ni las demás consideraciones económicas y las demás circunstancias que determinan procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en el artículo 19 fracción XIII del Reglamento Interior de la Secretaría de Economía, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número 0420/DJCC/2020.

GOBIERNO DE MÉXICO | IMSS



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

**a)** Proporcionar el servicio en las fechas o plazos y lugares específicos conforme a lo requerido en el presente contrato y anexos respectivos.

**b)** Correrá bajo su cargo los costos de flete, transporte, seguro y de cualquier otro derecho que se genere, hasta el lugar de la prestación del servicio, así como el costo de su traslado de regreso al término del presente contrato, en caso de aplicar.

**c)** Cumplir con las especificaciones técnicas y de calidad y demás condiciones establecidas en el presente contrato y respectivos anexos, así como la cotización y el requerimiento asociado a ésta;

**d)** Asumir su responsabilidad ante cualquier situación que pudiera generarse con motivo del presente contrato.

**e)** No difundir a terceros sin autorización expresa de **"EL INSTITUTO"** la información que le sea proporcionada, inclusive después de la rescisión o terminación del presente instrumento, sin perjuicio de las sanciones administrativas, civiles y penales a que haya lugar.

**f)** Proporcionar la información que le sea requerida por parte de la Secretaría de la Función Pública y el Órgano Interno de Control en **"EL INSTITUTO"**, de conformidad con el artículo 107 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

**"LAS PARTES"** que suscriben el presente contrato en su carácter de **"EL PROVEEDOR"**, asumen las obligaciones materia de este instrumento jurídico en forma *mancomunada* conforme a lo estipulado en el convenio de participación conjunta.

**OCTAVA. OBLIGACIONES DE "EL INSTITUTO".**

**a)** Otorgar todas las facilidades necesarias, a efecto de que **"EL PROVEEDOR"** lleve a cabo el objeto del presente contrato en los términos convenidos.

**b)** Sufragar el pago correspondiente en tiempo y forma, por la prestación del servicio.

**c)** Extender a **"EL PROVEEDOR",** en caso de que lo requiera, por conducto del administrador del presente contrato, la constancia de cumplimiento de obligaciones contractuales inmediatamente que se cumplan éstas a satisfacción expresa de dicho servidor público para que se dé trámite a la cancelación de la garantía de cumplimiento del presente contrato.

**NOVENA. LUGAR, PLAZOS 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 los plazos y en los lugares establecidos en el Anexo Técnico, en los Términos y Condiciones integrados en el **Anexo 2 (dos)** de este contrato, apegándose a las condiciones, alcances y características detalladas en la Convocatoria, Junta de Aclaraciones y Acta de Fallo, disponibles para su consulta en CompraNet y a lo ofrecido en sus propuestas técnica y económica que se agregan en el **Anexo 3 (tres).**

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado, precios de referencia, ni de aspectos técnicos, económicos y las demás circunstancias que determinaron precedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social con base en la Delegación de Facultades publicada en el Diario Oficial de la Federación el 30 de noviembre de 2010, en relación con el Acuerdo ACDO.SA2.HCT.250217/37 de la Comisión Jurídica, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número: DCONSULTA/2022/007

GOBIERNO DE MÉXICO

La prestación de los servicios iniciará a partir del día hábil siguiente a la notificación del fallo y hasta el 30 de septiembre de 2024.

Asimismo, se deberán observar los plazos establecidos en el Anexo Técnico y en los Términos y Condiciones que se agregan en el **Anexo 2 (dos)** del presente contrato.

**"EL PROVEEDOR"** deberá entregar al Titular de la División de Seguridad Informática Física dependiente de la Coordinación de Telecomunicaciones y Seguridad de la Información los entregables conforme a lo señalado en el Anexo Técnico y los Términos y Condiciones, que se agregan al presente contrato en el **Anexo 2 (dos).**

- La entrega se realizará en las instalaciones de **"EL INSTITUTO"** ubicadas en la Avenida Paseo de la Reforma 476, Anexo de Telecomunicaciones Planta Alta, Colonia Juárez, Demarcación Territorial Cuauhtémoc, Ciudad de México, C.P. 06600.
- El horario para la entrega será de las 9:00 horas a las 17:00 horas
- En caso de contingencia podrá solicitarse la entrega de las cartas requeridas en cualquiera de los inmuebles que formen parte de las Oficinas Centrales de **"EL INSTITUTO"**, ubicadas en la Colonia Juárez, Demarcación Territorial Cuauhtémoc, C.P. 06600 en la Ciudad de México.

**"EL PROVEEDOR"** convino en conjuntar sus recursos técnicos, legales, administrativos, económicos y financieros por lo que se obliga a prestar el servicio objeto del presente contrato en términos del convenio de participación conjunta.

**"EL PROVEEDOR"** conviene que en el supuesto de que cualquiera se declare en quiebra o suspensión de pagos, no los libera de cumplir con sus obligaciones, por lo que cualquiera de ellas que subsista, acepta y se obliga expresamente a responder de forma **mancomunada** las obligaciones contractuales a que hubiere lugar.

## DÉCIMA. NORMAS, LICENCIAS, AUTORIZACIONES Y PERMISOS.

El servicio objeto del presente contrato deberá 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 la Ley de Infraestructura de la Calidad; en su caso, con las normas de referencia o especificaciones técnicas y cumplir con las características y especificaciones requeridas en la Convocatoria, Anexo Técnico y los Términos y Condiciones, que se agregan al presente contrato en el **Anexo 2 (dos)**.

## DÉCIMA PRIMERA. CALIDAD DEL SERVICIO.

**"EL PROVEEDOR"**, deberá contar con la infraestructura necesaria, personal técnico especializado en el ramo, herramientas, técnicas y equipos adecuados para proporcionar el servicio requerido, a fin de garantizar que el objeto de este contrato sea proporcionado con la calidad, oportunidad y eficiencia requerida para tal efecto, comprometiéndose a realizarlo a satisfacción de **"EL INSTITUTO"** y con estricto apego a lo establecido en las cláusulas del



Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado realizada, ni de la procedencia y/o viabilidad de los aspectos técnicos, económicos y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en el artículo 19 fracción I, del Acuerdo por el que se delegan facultades en diversos servidores públicos del Instituto, en materia de Convenios, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Jurídicos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número 00DIR0CJC/2022/007

GOBIERNO DE MÉXICO | IMSS

presente instrumento jurídico y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta.

**"EL INSTITUTO"** no estará obligado a recibir los servicios cuando éstos no cumplan con los requisitos establecidos en el párrafo anterior.

**DÉCIMA SEGUNDA. DEFECTOS Y VICIOS OCULTOS.**

**"EL PROVEEDOR"** queda obligado ante **"EL INSTITUTO"** a responder de los defectos y vicios ocultos derivados de las obligaciones del presente contrato, así como de cualquier otra responsabilidad en que hubiere incurrido, en los términos señalados en este instrumento jurídico y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta, y/o en la legislación aplicable en la materia.

Para los efectos de la presente cláusula, se entiende por vicios ocultos los defectos que existan en el servicio que lo hagan impropio para los usos a que se le destine o que disminuyan de tal modo este uso, que de haberlo conocido **"EL INSTITUTO"** no lo hubiere adquirido o los hubiere adquirido a un precio menor.

**DÉCIMA TERCERA. RESPONSABILIDAD.**

**"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 lleguen a causar a **"EL INSTITUTO"**, con motivo de las obligaciones pactadas, o bien por los defectos o vicios ocultos en el servicio prestado, de conformidad con lo establecido en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

**DÉCIMA CUARTA. IMPUESTOS Y DERECHOS.**

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 prestación del servicio objeto de este contrato.



Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se hace responsable de la veracidad de la información proporcionada, ni se pronuncia sobre la viabilidad técnica, económica y financiera, ni sobre aspectos económicos y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con base en la delegación de facultades establecida en el Acuerdo por el que se delegan facultades en diversos servidores públicos del Instituto, para suscribir convenios, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número: DCJCNCO/0000/2022

GOBIERNO DE MÉXICO | IMSS

## DÉCIMA QUINTA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES.

**"EL PROVEEDOR"** no podrá ceder total o parcialmente los derechos y obligaciones derivados del presente contrato, a favor de cualquier otra persona física o moral, con excepción de los derechos de cobro, en cuyo caso se deberá contar con la conformidad previa y por escrito de **"EL INSTITUTO"** deslindando a ésta de toda responsabilidad.

## DÉCIMA SEXTA. DERECHOS DE AUTOR, 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 de propiedad industrial o intelectual a nivel Nacional o Internacional.

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

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

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

Asimismo, se deberán observar lo señalado en el numeral 16. de los Términos y Condiciones que se agregan en el **Anexo 2 (dos)** del presente contrato.

## DÉCIMA SÉPTIMA. CONFIDENCIALIDAD.

**"LAS PARTES"** están conformes en que la información que se derive de la celebración del presente instrumento jurídico, así como toda aquella información que **"EL INSTITUTO"** entregue a **"EL PROVEEDOR"** tendrá el carácter de confidencial, por lo que este se compromete, de forma directa o a través de interpósita persona, a no proporcionarla o divulgarla por escrito, verbalmente o por cualquier otro medio a terceros, inclusive después de la terminación de este contrato.

La información contenida en el presente contrato es pública, de conformidad con lo dispuesto en los artículos 70 fracción XXVIII de la Ley General de Transparencia y Acceso a la Información Pública y 68 de la Ley Federal de Transparencia y Acceso a la Información Pública; sin embargo, la información que proporcione **"EL INSTITUTO"** a **"EL PROVEEDOR"** para el



Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado, así como tampoco se pronuncia sobre la procedencia y/o viabilidad de los aspectos técnicos, económicos y las demás circunstancias que determinaron precedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en el artículo 19 fracción VII del Reglamento Interior de la Consejería Jurídica del Ejecutivo Federal, en consecuencia, se registró bajo el número 00/DCLC/0000/2020

GOBIERNO DE MÉXICO

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

cumplimiento del objeto materia del mismo, será considerada como confidencial en términos de los artículos 116 y 113, respectivamente, de los citados ordenamientos jurídicos, y 22, de la Ley del Seguro Social, por lo que **"EL PROVEEDOR"** se compromete a recibir, proteger y guardar la información confidencial proporcionada por **"EL INSTITUTO"** con el mismo empeño y cuidado que tiene respecto de su propia información confidencial, así como hacer cumplir a todos y cada uno de los usuarios autorizados a los que les entregue o permita acceso a la información confidencial, en los términos de este instrumento.

**"EL PROVEEDOR"** se compromete a que la información considerada como confidencial no será utilizada para fines diversos a los autorizados con el presente contrato; asimismo, dicha información no podrá ser copiada o duplicada total o parcialmente en ninguna forma o por ningún medio, ni podrá ser divulgada a terceros que no sean usuarios autorizados. De esta forma, **"EL PROVEEDOR"** se obliga a no divulgar o publicar informes, datos y resultados obtenidos objeto del presente instrumento, toda vez que son propiedad de **"EL INSTITUTO"**.

Cuando de las causas descritas en las cláusulas de **CAUSALES DE RESCISIÓN ADMINISTRATIVA DEL CONTRATO Y PROCEDIMIENTO DE RESCISIÓN** y **TERMINACIÓN ANTICIPADA**, del presente contrato, concluya la vigencia del mismo, subsistirá la obligación de confidencialidad sobre el servicio establecido en este instrumento legal.

En caso de incumplimiento a lo establecido en esta cláusula, **"EL PROVEEDOR"** tiene conocimiento en que **"EL INSTITUTO"** podrá ejecutar o tramitar las sanciones establecidas en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento, así como presentar las denuncias correspondientes de conformidad con lo dispuesto por el Libro Segundo, Título Noveno, Capítulos I y II del Código Penal Federal y demás normatividad aplicable.

De igual forma, **"EL PROVEEDOR"** se compromete a no alterar la información confidencial, a llevar un control de su personal y hacer de su conocimiento las sanciones que se aplicarán en caso de incumplir con lo dispuesto en esta cláusula, por lo que, en su caso, se obliga a notificar a **"EL INSTITUTO"** cuando se realicen actos que se consideren como ilícitos, debiendo dar inicio a las acciones legales correspondientes y sacar en paz y a salvo a **"EL INSTITUTO"** de cualquier proceso legal.

**"EL PROVEEDOR"** se obliga a poner en conocimiento de **"EL INSTITUTO"** cualquier hecho o circunstancia que en razón del servicio prestados sea de su conocimiento y que pueda beneficiar o evitar un perjuicio a la misma.

**"EL PROVEEDOR"** no podrá, con motivo del servicio que preste a **"EL INSTITUTO"**, utilizar la información a que tenga acceso, para asesorar, patrocinar o constituirse en consultor de cualquier persona que tenga relaciones directas o indirectas con el objeto de las actividades que lleve a cabo.

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se emite opinión alguna sobre aspectos técnicos, económicos y financieros, económicos y las demás circunstancias que determinaron procedentes la área requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en el artículo 19 fracción XXIII del Reglamento de Adquisiciones, Arrendamientos y Servicios del Sector Público, Convenios, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número DJ/DSSC/UACAOF/2019

GOBIERNO DE MÉXICO | IMSS



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

Asimismo, **"EL PROVEEDOR"** deberá observar lo establecido en los numerales 10 del Anexo Técnico y 15 de los Términos y Condiciones que se agregan en el **Anexo 2 (dos)** del presente contrato.

**DÉCIMA OCTAVA. ADMINISTRACIÓN, VERIFICACIÓN, SUPERVISIÓN Y ACEPTACIÓN DEL SERVICIO.**

**"EL INSTITUTO"** designa como responsable de administrar y vigilar el cumplimiento del presente contrato al C. Abraham Gutiérrez Castillo, Titular de la División de Seguridad Informática Física, con el objeto de verificar el óptimo cumplimiento del mismo, por lo que indicará a **"EL PROVEEDOR"** las observaciones que se estimen pertinentes, quedando éste obligado a corregir las anomalías que le sean indicadas, así como deficiencias en la prestación del servicio, de conformidad con lo establecido en el documento de designación de administrador del presente contrato que se agrega al presente 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 PRESENTE CONTRATO la persona que sustituya al servidor público en el cargo, conforme a la designación correspondiente.

Asimismo, **"EL INSTITUTO"** sólo aceptará el servicio materia del presente contrato y autorizará el pago del mismo previa verificación de las especificaciones requeridas, de conformidad con lo especificado en el presente contrato y sus correspondientes anexos, así como la cotización y el requerimiento asociado a ésta.

El servicio será recibido previa revisión del administrador del presente contrato; la inspección del servicio consistirá en la verificación del cumplimiento de las especificaciones técnicas establecidas en el contrato y en su caso en los anexos respectivos, así como la cotización y el requerimiento asociado a ésta.

En tal virtud, **"EL PROVEEDOR"** manifiesta expresamente su conformidad de que hasta en tanto no se cumpla con lo establecido en el párrafo anterior, el servicio no se tendrá por aceptado por parte de **"EL INSTITUTO"**.

**"EL INSTITUTO"**, a través del administrador del presente contrato o a través del personal que para tal efecto designe, podrá rechazar el servicio si no reúne las especificaciones y alcances establecidos en este contrato, en su Anexo Técnico y en los Términos y Condiciones, que se agregan al presente contrato en el **Anexo 2 (dos)**, obligándose **"EL PROVEEDOR"** en este supuesto a entregarlos nuevamente bajo su exclusiva responsabilidad y sin costo adicional para **"EL INSTITUTO"**.

**DÉCIMA NOVENA. DEDUCCIONES.**

Con fundamento en lo dispuesto en los artículos 53 Bis de la Ley de Adquisiciones,



Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se hace responsable de la información técnica, financiera, económica y las demás circunstancias que determinaron precedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción II, del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en los artículos 1, 2 fracción I, 3 fracción I, 4 fracción I, 5 fracción I, 6 fracción I, 7 fracción I, 8 fracción I, 9 fracción I, 10 fracción I, 11 fracción I, 12 fracción I, 13 fracción I, 14 fracción I,

Arrendamientos y Servicios del Sector Público y 97 de su Reglamento, **"EL PROVEEDOR"**, por la entrega parcial o deficiente en la prestación del servicio, se hará acreedor a una sanción por los conceptos y porcentajes señalados en el Anexo Técnico y en los Términos y Condiciones, que se agregan al presente contrato en el **Anexo 2 (dos)**.

El administrador del presente contrato será responsable del cálculo, aplicación y seguimiento de las deducciones. El monto máximo de aplicación de las deducciones no podrá 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 presente contrato.

**VIGÉSIMA. PENAS CONVENCIONALES.**

De conformidad con lo establecido en los artículos 45, fracción XIX, 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 95 y 96 de su Reglamento, la pena convencional aplicable a **"EL PROVEEDOR"**, por atraso en la prestación de los servicios será, sin considerar el I.V.A., por los conceptos, porcentajes y calculo establecidos en el Anexo Técnico y en los Términos y Condiciones, que se agregan al presente contrato en el **Anexo 2 (dos)**.

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 de la prestación 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.

**VIGÉSIMA PRIMERA. SANCIONES ADMINISTRATIVAS.**

Cuando **"EL PROVEEDOR"** incumpla con sus obligaciones contractuales por causas imputables a éste, y como consecuencia, cause daños y/o perjuicios graves a **"EL INSTITUTO"**, o bien, proporcione información falsa, actúe con dolo o mala fe en la celebración del presente contrato o durante la vigencia del mismo, por determinación de la Secretaría de la Función Pública, se podrá hacer acreedor a las sanciones establecidas en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en los términos de los artículos 59, 60 y 61 de dicho ordenamiento legal y 109 al 115 de su Reglamento.

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se pronuncia sobre la viabilidad técnica, económica, financiera, jurídica, económicas y las demás circunstancias que determinan precedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en los artículos 1, 2 fracción I, 3 fracción I, 4 fracción I, 5 fracción I, 6 fracción I, 7 fracción I, 8 fracción I, 9 fracción I, 10 fracción I, 11 fracción I, 12 fracción I, 13 fracción I, 14 fracción I,

## VIGÉSIMA SEGUNDA. SANCIONES APLICABLES Y TERMINACIÓN DE LA RELACIÓN CONTRACTUAL

**"EL INSTITUTO"**, de conformidad con lo establecido en los artículos 53, 53 Bis, 54 y 54 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 86 segundo párrafo, 95 al 100 y 102 de su Reglamento, aplicará sanciones, o en su caso, llevará a cabo la cancelación de partidas total o parcialmente o la rescisión administrativa del presente contrato.

## VIGÉSIMA TERCERA. EXCLUSIÓN LABORAL.

**"LAS PARTES"** convienen en que **"EL INSTITUTO"** no adquiere ninguna obligación de carácter laboral con **"EL PROVEEDOR"** ni con los elementos que este utilice para la prestación del servicio objeto del presente contrato, por lo cual no se le podrá considerar como patrón ni como un sustituto. En particular el personal se entenderá relacionado exclusivamente con la o las personas que lo emplearon y por ende cada una de ellas asumirá su responsabilidad por dicho concepto.

Igualmente, y para este efecto y cualquiera no previsto, **"EL PROVEEDOR"** exime expresamente a **"EL INSTITUTO"** de cualquier responsabilidad laboral, civil, penal, de seguridad social o de otra especie que, en su caso, pudiera llegar a generarse; sin embargo, si **"EL INSTITUTO"** tuviera que realizar alguna erogación por alguno de los conceptos que anteceden, **"EL PROVEEDOR"** se obliga a realizar el reembolso e indemnización correspondiente.

Por lo anterior, **"LAS PARTES"** reconocen expresamente en este acto que **"EL INSTITUTO"** no tiene nexo laboral alguno con **"EL PROVEEDOR"**, por lo que éste último libera a **"EL INSTITUTO"** de toda responsabilidad relativa a cualquier accidente o enfermedad que pudiera sufrir o contraer cualquiera de sus trabajadores durante el desarrollo de sus labores o como consecuencia de ellos, así como de cualquier responsabilidad que resulte de la aplicación de la Ley Federal del Trabajo, de la Ley del Seguro Social, de la Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores y/o cualquier otra aplicable, derivada de la prestación del servicio materia de este contrato.

## VIGÉSIMA CUARTA. SUSPENSIÓN DE LA PRESTACIÓN DEL SERVICIO.

Cuando en la prestación del servicio, se presente caso fortuito o de fuerza mayor, **"EL INSTITUTO"** bajo su responsabilidad, podrá de resultar aplicable conforme a la normatividad en la materia, suspender el servicio, en cuyo caso únicamente se pagarán aquellos que hubiesen sido efectivamente recibidos por **"EL INSTITUTO".**

Cuando la suspensión obedezca a causas imputables a **"EL INSTITUTO"**, a solicitud escrita de **"EL PROVEEDOR"**, cubrirá los gastos no recuperables, durante el tiempo que dure esta suspensión, para lo cual **"EL PROVEEDOR"** deberá presentar dentro de los 30 (treinta) días naturales siguientes de la notificación del término de la suspensión, el CFDI y documentación

Dirección Jurídica
Unidad de Asistencia Consultiva y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se pronuncia sobre aspectos técnicos, económicos, financieros o de costos, ni sobre las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente instrumento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en el artículo 19 fracción I, del Reglamento de Adquisiciones, Arrendamientos y Servicios del Sector Público, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número: DJ/DCSC/UACyAOF/0207

GOBIERNO DE MÉXICO | IMSS

de los gastos no recuperables en que haya incurrido, siempre que estos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente contrato.

**"EL INSTITUTO"** pagará los gastos no recuperables, en moneda nacional (pesos mexicanos), dentro de los 45 (cuarenta y cinco) días naturales posteriores a la presentación de la solicitud debidamente fundada y documentada de "**EL PROVEEDOR**", así como del CFDI o factura electrónica respectiva y documentación soporte.

En caso de que **"EL PROVEEDOR"** no presente en tiempo y forma la documentación requerida para el trámite de pago, la fecha de pago se recorrerá el mismo número de días que dure el retraso.

El plazo de suspensión será fijado por **"EL INSTITUTO"**, a cuyo término en su caso, podrá iniciarse la terminación anticipada del presente contrato, o bien, podrá continuar produciendo todos los efectos legales, una vez que hayan desaparecido las causas que motivaron dicha suspensión.

**VIGÉSIMA QUINTA. CAUSALES DE RESCISIÓN ADMINISTRATIVA DEL PRESENTE CONTRATO Y PROCEDIMIENTO DE RESCISIÓN.**

**"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 el Anexo Técnico, Términos y Condiciones, que se agregan al presente contrato en el **Anexo 2 (dos)**, y las que se señalan a continuación:

1. Cuando no entregue la garantía de cumplimiento del presente contrato, a más tardar dentro de los 10 (diez) días naturales 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 se compruebe que **"EL PROVEEDOR"** haya prestado el servicio con descripciones y características distintas a las pactadas en este contrato o cuando no los entregue conforme a las normas y/o calidad solicitadas por **"EL INSTITUTO".**
4. Cuando se transmitan total o parcialmente, bajo cualquier título y a favor de otra persona física o moral, los derechos y obligaciones a que se refiere el presente documento, con excepción de los derechos de cobro, previa autorización de **"EL INSTITUTO"**.
5. Si la autoridad competente declara el concurso mercantil o cualquier situación análoga o equivalente que afecte el patrimonio de **"EL PROVEEDOR"**.
6. Cuando de manera reiterativa y constante, **"EL PROVEEDOR"** sea sancionado por parte de **"EL INSTITUTO"** con penalizaciones y/o deducciones sobre el mismo concepto del servicio proporcionado, o por ubicarse en los límites de incumplimientos previstos en la cláusula de penas convencionales y/o deducciones del presente instrumento.

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación y/o viabilidad de los aspectos técnicos, económicos y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en el artículo 19 fracción VII del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, Convenios, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número: DJ/DUACAF/CLC/0000/2020

GOBIERNO DE MÉXICO



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

7. Cuando se incumplan o contravengan las disposiciones de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su reglamento y los demás lineamientos que rigen en la materia.

8. 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 la Ley Federal de Competencia Económica y artículo 34 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

9. Si **"EL PROVEEDOR"** no permite a **"EL INSTITUTO"** la administración y verificación a que se refiere la cláusula correspondiente señalada en el presente contrato.

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

**"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 presente cláusula, 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 aplicará 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 del presente contrato.



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

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se pronuncia sobre la suficiencia presupuestal, ni sobre los aspectos técnicos, económicos y las demás circunstancias que determinen procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en los artículos 2, fracción I, 3, fracción I, 4, fracción I, del Reglamento Interior de la Comisión, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registra bajo el número: DCJDJDCAOF/2020/07

GOBIERNO DE MÉXICO

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"** proporciona 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.

## VIGÉSIMA SEXTA. TERMINACIÓN ANTICIPADA.

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.

## VIGÉSIMA SÉPTIMA. DISCREPANCIAS.

**"LAS PARTES"** convienen que, en caso de discrepancia entre la Convocatoria y/o solicitud de cotización, la propuesta económica de **"EL PROVEEDOR"** y el presente contrato, prevalecerá



Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se pronuncia sobre la procedencia técnica y económica de los montos económicos y las demás circunstancias que determinan procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en los artículos 19 fracción XXIII y 20 fracción XXIII del Acuerdo que delega facultades en los titulares de las Coordinaciones, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número: DGDDSC/AJOD/2019/007

GOBIERNO DE MÉXICO | IMSS

lo establecido en la Convocatoria y/o solicitud de cotización, junta de aclaraciones respectiva, en caso de aplicar, de conformidad con lo dispuesto por el artículo 81 fracción IV, del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

## VIGÉSIMA OCTAVA. CONCILIACIÓN.

**"LAS PARTES"** acuerdan que para el caso de que se presenten desavenencias derivadas de la ejecución y cumplimiento del presente contrato se someterán al procedimiento de conciliación establecido en los artículos 77, 78, 79 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 126 al 136 de su Reglamento y al Decreto por el que se establecen las acciones administrativas que deberá implementar la Administración Pública Federal para llevar a cabo la conciliación o la celebración de convenios o acuerdos previstos en las leyes respectivas como medios alternativos de solución de controversias, publicado en el Diario Oficial de la Federación el 29 de abril de 2016.

La solicitud de conciliación se presentará mediante escrito, el cual contendrá los requisitos contenidos en el artículo 15 de la Ley Federal de Procedimiento Administrativo, además, hará referencia al número de contrato, al servidor público encargado de su administración, objeto, vigencia y monto del contrato, señalando, en su caso, sobre la existencia de convenios modificatorios, debiendo adjuntar copia de los instrumentos consensuales debidamente suscritos.

## VIGÉSIMA NOVENA. DOMICILIOS.

**"LAS PARTES"** señalan como sus domicilios legales para todos los efectos a que haya lugar y que se relacionan en el presente contrato, los que se indican en el apartado de Declaraciones, por lo que cualquier notificación judicial o extrajudicial, emplazamiento, requerimiento o diligencia que en dichos domicilios se practique, será enteramente válida, al tenor de lo dispuesto en el Título Tercero del Código Civil Federal y sus correlativos en los Estados de la República Mexicana.

## TRIGÉSIMA. LEGISLACIÓN APLICABLE.

**"LAS PARTES"** se obligan a sujetarse estrictamente para la prestación del servicio objeto del presente contrato a todas y cada una de las cláusulas que lo integran, así como la cotización y el requerimiento asociado a ésta, a la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento; al Código Civil Federal; la Ley Federal de Procedimiento Administrativo; al Código Federal de Procedimientos Civiles; a la Ley Federal de Presupuesto y Responsabilidad Hacendaria y su Reglamento, el Acuerdo por el que se expide el protocolo de actuación en materia de contrataciones públicas, otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones y a las demás disposiciones jurídicas aplicables.

## TRIGÉSIMA PRIMERA. JURISDICCIÓN.

**"LAS PARTES"** convienen que, para la interpretación y cumplimiento de este contrato, así como para lo no previsto en el mismo, se someterán a la jurisdicción y competencia de los



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

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado realizada, así como de la viabilidad de los aspectos técnicos, económicos y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con fundamento en el artículo 19 fracción XXIII del Acuerdo por el que se delegan facultades en diversos servidores públicos del Instituto, así como a los Convenios, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número DICONSULTA/2020/

GOBIERNO DE MÉXICO

Tribunales Federales en la Ciudad de México, renunciando expresamente al fuero que pudiera corresponderles en razón de su domicilio actual o futuro.

## FIRMANTES O SUSCRIPCIÓN.

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 cuadruplicado, en la Ciudad de México, el **19 de octubre de 2022**, quedando un ejemplar en poder de **"EL PROVEEDOR"** y los restantes en poder de **"EL INSTITUTO"**.

**POR "EL INSTITUTO"**
**INSTITUTO MEXICANO DEL SEGURO SOCIAL**
De conformidad con lo dispuesto por el artículo 277 F, cuarto párrafo, de la Ley del Seguro Social

**MTRO. ZOÉ ALEJANDRO ROBLEDO ABURTO**
Director General
R.F.C.: [redacted]

Interviene de conformidad con los artículos 6, fracción I, 8, párrafo primero y 69, fracción I, del Reglamento Interior del Instituto Mexicano del Seguro Social, en relación con el artículo 277 F, de la Ley del Seguro Social, así como del numeral 7.1 del Manual de Organización de la Dirección de Administración en relación con el artículo 268 A, de la Ley del Seguro Social

Interviene, de conformidad con el artículo 69, último párrafo del Reglamento Interior del Instituto Mexicano del Seguro Social; así como del numeral 7.1.3 del Manual de Organización de la Dirección de Administración en relación con el artículo 268 A, de la Ley del Seguro Social

**LIC. BORSALINO GONZÁLEZ ANDRADE**
Titular de la Dirección de Administración
R.F.C.: [redacted]

**MTRO. FERNANDO LORENZANA ROJAS**
Titular de la Unidad de Adquisiciones
R.F.C [redacted]

**SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: RFC, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN I Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016**



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

SIN TEXTO

Interviene de conformidad con los artículos 6, fracción I y 74 del Reglamento Interior del Instituto Mexicano del Seguro Social; numeral 7.1, del Manual de Organización de la Dirección de Innovación y Desarrollo Tecnológico en relación con el artículo 268 A, de la Ley del Seguro Social

**MTRA. CLAUDIA LAURA VÁZQUEZ ESPINOZA**
Titular de la Dirección de Innovación y Desarrollo Tecnológico
R.F.C. [redacted]

**C. FLORENCIO FERNANDO GONZÁLEZ VELÁZQUEZ**
Coordinador de Telecomunicaciones y Seguridad de la Información
R.F.C. [redacted]

**ADMINISTRADOR DEL CONTRATO**

**C. ABRAHAM GUTIÉRREZ CASTILLO**
Titular de la División de Seguridad Informática Física
R.F.C. [redacted]

Dirección Jurídica
Unidad de Asuntos Contenciosos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin prejuzgar sobre la justificación, procedimiento, términos y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se pronuncia sobre la presencia y/o calidad de los anexos técnicos, mismos que son responsabilidad de las áreas requirentes, técnica y/o contratante.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la División Jurídica en Compras y Contratación de Bienes y Servicios, en la fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con base en el dictamen elaborado por la División de Dictamen Jurídico de Contratos y Convenios y la Coordinación de Legislación y Consulta de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número: DC/DDJC/ADQ/2021/07

GOBIERNO DE MÉXICO

**SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: RFC, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN I Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016**



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

SIN TEXTO

**POR "EL PROVEEDOR"**
**OPERBES, S.A. DE C.V.**
R.F.C.: OPE070326DNA
(Participante A)

**C. LUIS ALBERTO DE LA GARZA AGUIRRE**
Representante Legal

**C. CESAR GERÓNIMO JIMÉNEZ CERVANTES**
Representante Legal

**SILENT4BUSINESS, S.A. DE C.V.**
R.F.C.: SIL160727HV7
(Participante B)

**BUFETE EMPRESARIAL GTI, S.A. DE C.V.**
R.F.C.: BEG141128JD5
(Participante C)

**C. GERARDO GARIBAY AYMES**
Representante Legal

**C. JUAN LUIS PINEDA GONZÁLEZ**
Representante Legal

*RRSR/HRJ/LBGP/CMBS*

Dirección Jurídica
Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores
Coordinación de Legislación y Consulta

La validación jurídica se efectúo sin prejuzgar sobre la justificación, procedimiento, término y condiciones de la contratación, ni del resultado de la investigación de mercado correspondiente, ni se pronuncia sobre la procedencia y/o viabilidad de los aspectos técnicos, económicos y las demás circunstancias que determinaron procedentes las áreas requirente, técnica y/o contratante.

GOBIERNO DE MÉXICO

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 fracción III, del Reglamento Interior del Instituto Mexicano del Seguro Social, con base en el dictamen elaborado por la Dirección de Dictamen Jurídico de Contratos y Convenios, de la Coordinación de Legislación y Consulta, de la Unidad de Asuntos Consultivos y de Atención a Órganos Fiscalizadores. En consecuencia, se registró bajo el número: DC/DDJCC/ADQ/2022/007



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

SIN TEXTO

| | | |
|---|---|---|
| IMSS | INSTITUTO MEXICANO DEL SEGURO SOCIAL<br>DIRECCIÓN DE ADMINISTRACIÓN<br>UNIDAD DE ADQUISICIONES<br>COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS<br>COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS | CONTRATO NÚMERO<br>019E18222-001 |

# ANEXO 1 (UNO)

## "DICTAMEN DE DISPONIBILIDAD PRESUPUESTAL PREVIO Y ACUERDO DEL H. CONSEJO TÉCNICO"

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

INSTITUTO MEXICANO DEL SEGURO SOCIAL

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

FOLIO: 0000439264-2022

[ ] Dictamen de Inversión
[X] Dictamen de Gasto

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

Concepto: OF. 1553 RECIBIDO EL 05/10/2022 "SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA 2022-2024 PARTIDA1"

Fecha Elaboración: 06/10/2022

Total Comprometido (en pesos): $ 50,487,311.44
Cuenta: 42062493 Serv Int Infraestructura Compu Unidad de Información: 099001 Centro de Costos: 500000
Partida Presupuestaria SHCP: 31904 Servicios integrales de infraestructura de cómputo

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 | 0.0 | 0.0 | 0.0 | 0.0 | 25,243.7 | 25,243.7 |

DISPONIBLE (en miles de pesos):

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |

El presente documento de existencia de respaldo presupuestario se emite en términos de lo señalado en el numeral 7.5.9.4 de la Norma Presupuestaria del Instituto Mexicano del Seguro Social (IMSS), y de lo establecido en el artículo 8°, 144 y 148 del Reglamento Interior del IMSS, es responsabilidad del área solicitante el destino y aplicación de los recursos. También se informa que este documento únicamente tendrá validez para el ejercicio fiscal en curso, y que con base en la revisión que se efectuó en el Sistema Financiero PREI-Millenium, en el Módulo de Control de Compromisos, en la combinación unidad de información y centro de costos, los montos señalados quedan comprometidos para dar inicio a las gestiones de adquisición de bienes y servicios con base al marco normativo vigente.

ATENTAMENTE

Lic. Jessica Miranda Vega

Titular Div de Ctrl y Seguimiento al Ppto de Oper en Ámbito Central

| DIA | MES | AÑO |
|---|---|---|
| | | |

DICTAMINADO DEFINITIVO

DICTAMEN DEFINITIVO

CONTRATO No. _____

IMPORTE DEFINITIVO (EN PESOS) : $ _____ .00

Clave: 6170-009-001

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

GOBIERNO DE MÉXICO

IMSS

*Secretaría del H. Consejo Técnico*

México 2021 Año de la Independencia

Of N°09/9001/030000/ 2076

Ciudad de México, 27 de octubre de 2021.

*H. Consejo Técnico*

Mtra. Claudia Laura Vázquez Espinoza
Directora de Innovación y Desarrollo Tecnológico

El H. Consejo Técnico, en la sesión ordinaria celebrada el día 27 de octubre del presente año, dictó el Acuerdo **ACDO.AS3.HCT.271021/266.P.DIDT,** en los siguientes términos:

"Este Consejo Técnico, con fundamento en lo dispuesto por los artículos 251 fracciones IV, V y XXXVII, 263 y 264 fracciones III, XIV y XVII, y 277 F de la Ley del Seguro Social; 5 y 57 de la Ley Federal de las Entidades Paraestatales; 31 fracción XX del Reglamento Interior del Instituto Mexicano del Seguro Social; de conformidad con el planteamiento presentado por el Director General, por conducto de la persona Titular de la Dirección de Innovación y Desarrollo Tecnológico, en términos del oficio número 117 del 18 de octubre de 2021; así como de los dictámenes de los Comités de Innovación y Desarrollo Tecnológico, y de Presupuesto del propio Órgano de Gobierno, emitidos en reuniones celebradas el 18 y 25 del mes y año citados, respectivamente, **Acuerda: Primero.-** Autorizar que la Dirección de Innovación y Desarrollo Tecnológico lleve a cabo la contratación plurianual, por un período de 42 meses, de los Servicios Administrados de Seguridad Informática y Comunicaciones, por un monto global máximo de hasta $465'401,064.24 (CUATROCIENTOS SESENTA Y CINCO MILLONES CUATROCIENTOS UN MIL SESENTA Y CUATRO PESOS 24/100 M.N.), incluido el Impuesto al Valor Agregado, con la distribución anual siguiente: **a)** en el ejercicio fiscal 2021, la cantidad de $11'080,977.72 (ONCE MILLONES OCHENTA MIL NOVECIENTOS SETENTA Y SIETE PESOS 72/100 M.N.); **b)** en el ejercicio fiscal 2022, la cantidad de $132,971,732.64 (CIENTO TREINTA Y DOS MILLONES NOVECIENTOS SETENTA Y UN MIL SETECIENTOS TREINTA Y DOS PESOS 64/100 M.N.); **c)** en el ejercicio fiscal 2023, la cantidad de $132,971,732.64 (CIENTO TREINTA Y DOS MILLONES NOVECIENTOS SETENTA Y UN MIL SETECIENTOS TREINTA Y DOS PESOS 64/100 M.N.); **d)** en el ejercicio fiscal 2024, la cantidad de $132'971,732.64 (CIENTO TREINTA Y DOS MILLONES NOVECIENTOS SETENTA Y UN MIL SETECIENTOS TREINTA Y DOS PESOS 64/100 M.N.); **e)** y en el ejercicio fiscal 2025, la cantidad de $55,404,888.60 (CINCUENTA Y CINCO MILLONES CUATROCIENTOS CUATRO MIL OCHOCIENTOS OCHENTA Y OCHO PESOS 60/100 M.N.). **Segundo.-** Instruir a la Dirección de Finanzas para que considere, dentro del

...vta.

ANEXOS
DIVISIÓN DE CONTRATOS

presupuesto de operación a partir del año 2022, en cada ejercicio fiscal, las cantidades correspondientes al periodo contratado, de conformidad con el punto Primero de este Acuerdo, quedando sujetas a la disponibilidad presupuestaria del ejercicio de que se trate, en cumplimiento a lo dispuesto por los artículos 24 y 25 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 32 y 50 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; así como 277 F y 277 G de la Ley del Seguro Social. **Tercero.-** La presente autorización se limita, exclusivamente, al ámbito presupuestario y no genera implicación alguna sobre los respectivos procedimientos de contratación, que deberán llevar a cabo los servidores públicos responsables, con estricto apego a lo establecido en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento; las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social; y las demás disposiciones que resulten aplicables, conforme a lo establecido en el artículo 277 G de la Ley del Seguro Social. **Cuarto.-** Instruir a la Dirección de Innovación y Desarrollo Tecnológico para que informe a este Órgano de Gobierno semestralmente, sobre el avance de los resultados de la contratación plurianual a que se refiere el presente Acuerdo, así como su cumplimiento. **Quinto.-** Instruir a la Dirección de Innovación y Desarrollo Tecnológico para que someta a consideración y aprobación de este órgano de Gobierno las modificaciones que pudiera requerir esta autorización, privilegiando la continuidad y fortalecimiento de los Servicios Administrados de Seguridad Informática y Comunicaciones".

Lo que comunico a usted para su conocimiento.

Atentamente,

**Lic. Marcos Bucio Mújica**
Secretario del H. Consejo Técnico.

Con copia:

- Mtro. Zoé Robledo Aburto. Director General y Presidente del H. Consejo Técnico.
- Mtra. Luisa María Alcalde Luján. Secretaria del Trabajo y Previsión Social y Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el Sistema Integral de Control de Acuerdos (SICA).*
- Dr. Rogelio Eduardo Ramírez de la O. Secretario de Hacienda y Crédito Público y Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el SICA.*
- Dr. Jorge Carlos Alcocer Varela. Secretario de Salud y Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el SICA.*

- Lic. Alejandro Salafranca Vázquez. Encargado del Despacho de la Subsecretaría del Trabajo de la Secretaría del Trabajo y Previsión Social y Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el SICA.*
- Dr. Hugo López-Gatell Ramírez. Subsecretario de Prevención y Promoción de la Salud, de la Secretaría de Salud y Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el SICA.*
- Lic. Omar Antonio Nicolás Tovar Ornelas. Director General de Programación y Presupuesto "A" de la Subsecretaría de Egresos de la Secretaría de Hacienda y Crédito Público y Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el SICA.*
- Sr. José Abugaber Andonie. Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el SICA.*
- Ing. José Héctor Tejada Shaar. Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el SICA.*
- Ing. Salomón Presburger Slovik. Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el SICA.*
- Dr. Manuel Reguera Rodríguez. Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el SICA.*
- Sr. José Luis Carazo Preciado. Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el SICA.*
- Mtro. Rodolfo Gerardo González Guzmán. Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el SICA.*
- Sr. José Noé Mario Moreno Carbajal. Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el SICA.*
- Sr. Sergio Beltrán Reyes. Miembro del H. Consejo Técnico. *La copia podrá ser descargada en el SICA.*
- Mtro. Borsalino González Andrade. Director de Administración.
- Mtro. Marco Aurelio Ramírez Corzo. Director de Finanzas.

---

- Mtra. María Fernanda Heraldez Ríos. Coordinadora de Órganos de Gobierno.
- Lic. Gustavo A. Zavala Guerrero. Coordinador Técnico de Órganos Superiores. *La copia será enviada por el Sistema Institucional de Control de Gestión de Correspondencia (SICGC).*

GAZG/JACM/MACG/

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

| | | |
|---|---|---|
| IMSS | INSTITUTO MEXICANO DEL SEGURO SOCIAL<br>DIRECCIÓN DE ADMINISTRACIÓN<br>UNIDAD DE ADQUISICIONES<br>COORDINACIÓN DE ADQUISICIÓN DE BIENES Y<br>CONTRATACIÓN DE SERVICIOS<br>COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS | CONTRATO<br>NÚMERO<br>019E18222-001 |

# ANEXO 2 (DOS)

# "ANEXO TÉCNICO y TÉRMINOS Y CONDICIONES"

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

## Anexo 1.- Anexo Técnico

### 1. Objetivo del Documento

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

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

### 1.1. Objetivo General

Contar, de manera integrada y unificada, con los servicios administrados mediante dos partidas que garanticen la continuidad operativa, de negocio y de seguridad de la información del IMSS mediante: (1) Toma en operación y transición, (2) servicios de infraestructura que operen, den soporte y mantenimiento a la infraestructura instalada, y que, implementen y gestionen infraestructura para los centros de datos y den la atención a los servicios y aplicaciones con las que cuenta el instituto, (3) servicios que brinden protección a servidores, aplicaciones y bases de datos mediante una solución integral, (4) servicios de seguridad de la información, en materias específicas relacionadas con las tecnologías de la información, comunicaciones y seguridad de la información, incluyendo servicios especializados.

### 1.2. Objetivos Específicos

- Asegurar y proteger la información Institucional.
- Garantizar la continuidad operativa, de negocio y de la seguridad de la información de la Institución, durante la vigencia del presente contrato, especialmente durante la toma de operación y transición del contrato anterior a los servicios propios de SASI 2022-2024.
- Fortalecer la seguridad de la información de la Institución contra amenazas, disminuyendo el riesgo de sufrir incidentes de seguridad, mediante el uso de tecnología de punta para el monitoreo, detección, aseguramiento, contención y respuesta ante ataques que puedan presentarse en la infraestructura de cómputo, sistemas y aplicaciones del IMSS.
- Contar con servicios de infraestructura regulados por niveles de servicio, que: implementen (instalen, migren, habiliten y pongan a punto) los componentes necesarios en los centros de datos y servicios propios del IMSS y que de forma complementaria gestionen (operen, monitoreen, den soporte y mantenimiento preventivo y correctivo) a la correspondiente infraestructura con el propósito de satisfacer las necesidades de: conectividad, comunicación, protección, control y filtrado de la propia Institución, manteniendo la plataforma tecnológica en condiciones óptimas de operación.
- Contar con los servicios de protección de forma unificada e integrada, incluyendo prevención de pérdida de información, protección de computo físico o virtual, protección de correo electrónico externo e interno, herramientas de colaboración y trazabilidad, filtrado e inspección de acceso a internet e intranet, mediante una solución integral que permita una gestión consolidada de las funcionalidades, características y servicios, con el propósito de mantener, asegurar y robustecer el esquema de seguridad del IMSS.
- Contar con servicios de seguridad de la información, que complementen el esquema de seguridad institucional de forma consistente y robusta, con el control, aseguramiento, diagnóstico, pruebas, metodologías, de distintos rubros como el de acceso a cuentas privilegiadas, base de datos, aplicaciones, fuentes múltiples de información para correlación y trazabilidad de eventos,

vulnerabilidades, investigación forense y de procesos de seguridad, así como con otros servicios especializados en materia de seguridad y tecnologías de la información.
- Contar con servicios para la gestión del cambio y de soporte extendido que tienen como objetivo coadyuvar en la prestación del resto de los servicios SASI 2022-2024.

## 2. Alcance

El alcance del SASI 2022-2024 incluye:

- Un esquema de servicios de implementación, gestión y monitoreo de la infraestructura física, de seguridad necesaria para integrar los centros de datos mediante una arquitectura flexible y que responda a las necesidades de migración. Este esquema incluye la operación, soporte y mantenimiento de la infraestructura instalada, así como su potencial substitución, con el fin de mantener una plataforma moderna, y uniforme tecnológicamente, que garantice la continuidad operativa, del negocio y de la seguridad de la información del IMSS.
- Un esquema de servicios de protección con una solución integral que incluya: protección de servicios de colaboración internos, correo externo y navegación web, detecte y proteja contra amenazas avanzadas, prevenga la fuga de información y mediante una gestión consolidada.
- Un esquema de servicios de seguridad que complementen el esquema de protección, mediante servicios orientados a: Firewalls, IPS, Filtrado de Contenido, Anti DDoS, Antispam, WAF, DBF, VPN, así como la implementación y administración de nuevos servicios que requiera el instituto, como son análisis de vulnerabilidades, análisis forense, pruebas de penetración, borrado seguro de información, aseguramiento de aplicaciones, ciberinteligencia (ciberseguridad), servicios de protección en redes inalámbricas y seguridad en dispositivos móviles, servicios de gestión y control de acceso para usuarios privilegiados (AAA), servicio de correlación de eventos, servicio de protección de amenazas persistentes avanzadas (APT), servicios de gestión de procesos de seguridad y servicios especializados en materia de seguridad de la información, de este modo, se tiene un esquema de seguridad completo.

## 3. Beneficios

Los beneficios que se esperan alcanzar con la prestación de los servicios SASI 2022-2024 se dirigen a garantizar la continuidad de la operación, del negocio y de la seguridad de la información de la propia Institución, fortaleciendo su esquema de infraestructura, comunicaciones, servicios de protección y en servicios especializados en materia de seguridad de la información, contribuyendo al cumplimiento de los objetivos del IMSS; extendiéndose a toda la institución en términos técnicos, protección y servicios especializados como son:

- Contar con una infraestructura física, de seguridad, flexible y escalable; basada en una arquitectura que se adapte oportunamente a las necesidades de migración y a las exigencias para la prestación de los servicios que demanda el IMSS.
- Proporcionar una plataforma tecnológicamente moderna y estandarizada que se mantenga actualizada y en buenas condiciones, para el despliegue oportuno de los servicios que garanticen la continuidad operativa, de negocios y de seguridad de la información del IMSS.
- Contar con un esquema completo de servicios especializados en materia de tecnologías de la información que dé protección tanto a la infraestructura, a los servicios y a los usuarios finales tanto como a aspectos normativos, de procesos, de calidad y de ingeniería entorno a la seguridad de la información.

- Proporcionar los servicios de protección para los usuarios, a través de un esquema desde la red interna y desde la red externa ante los elementos de riesgo y perniciosos que pueden presentarse.
- Garantizar la calidad en la entrega de los servicios de SASI 2022-2024 mediante Acuerdos de Niveles de Servicio elaborados considerando el impacto que genera su no disponibilidad o la no entrega de esos servicios en el esquema de seguridad completo de SASI 2022-2024.

**4. Actualización Tecnológica**

Como parte de su proceso de evolución tecnológica, el IMSS se reserva el derecho de actualizar las especificaciones de infraestructura, de *software* y *hardware* que mantienen los servicios de SASI 2022-2024, toda vez que los activos de infraestructura son susceptibles de integrar mejoras en hardware o software, lo que permite proveer mecanismos de protección adicional conforme la evolución de funcionalides en materia de seguridad o para aquellos que requieran de una sustitución (por falla) o un reajuste. Por lo tanto, el "LICITANTE" conoce y acepta que el IMSS está en continua evolución tecnológica, por lo que se debe apegar a ella en todo momento.

Como parte de su proceso de evolución tecnológica, el IMSS se reserva el derecho de actualizar las especificaciones de infraestructura, de *software* y *hardware* que mantienen los servicios de SASI 2022-2024, con el objetivo de proteger a la Institución de la obsolescencia, conforme a la misma evolución del mercado observando el mapa de ruta de actualización de los componentes, para los servicios SASI 2022-2024, solicitados o para aquellos que requieran de una sustitución (por falla) o un reajuste. Por lo tanto, el "LICITANTE" conoce y acepta que el IMSS está en continua evolución tecnológica, por lo que se debe apegar a ella en todo momento.

El "LICITANTE", tomando en consideración las características del servicio, deberá cumplir con los mecanismos de seguridad de la información o controles que le establezca la Coordinación de Telecomunicaciones y Seguridad de la Información, con la finalidad de garantizar la conservación, integridad, confiabilidad y disponibilidad de los datos que se encuentran en los sistemas tecnológicos del IMSS una vez que haya iniciado la prestación del servicio, en caso de incumplimiento, el "LICITANTE" deberá considerar lo establecido en el apartado de "Penas Convencionales y Deducciones".

El "LICITANTE" efectuará la actualización de cualquier tipo de licencia, componente, dispositivo, parche, arquitectura, etc. siempre y cuando el fabricante de dicho componente haya liberado una versión que lo reemplace por aspectos de seguridad, compatibilidad, fin de soporte, capacidad, error o falla detectada, o similar; con la finalidad de mantener estable y segura la operación de los servicios SASI 2022-2024. Toda actualización o mejora deberá ser consultada y aprobada por el IMSS. Estos mecanismos le garantizarán a la institución que, durante toda la vigencia del contrato, dispondrá de los componentes del servicio que incorporan la versión más avanzada de la tecnología validada, probada y liberada por los fabricantes, para satisfacción de las necesidades del servicio SASI 2022-2024.

Los plazos para llevar a cabo las actualizaciones tecnológicas de nuevas versiones (*software*) de los componentes relacionados con los servicios de SASI 2022-2024 serán de, por lo menos, seis meses después de su última versión liberada por el fabricante, siempre que el IMSS consid ere que dicha actualización es conveniente para alcanzar los objetivos de SASI 2022-2024 y del propio IMSS, durante la vigencia del contrato, buscando reducir el riesgo e impacto a la operación, al ejecutar estas actualizaciones siempre se deberá contar con un documento de recomendaciones y riesgos generado por los ingenieros del fabricante al igual se deberá contar con apoyo del centro de asistencia técnica del fabricante durante las ventanas de ejecución de cambios.

**5. Requerimientos del servicio**

Los Servicios requeridos y que deberán ser parte de la solución propuesta, se desagregan por partida, mismos que deberán incluir al menos lo siguiente:

## Partida 1

1. **Servicios de Seguridad - Continuidad Operativa**
   (Firewalls, IPS, AntiDDoS, Filtrado Web, Filtrado de correo, Firewall de Aplicaciones WEB, Firewall de base de datos, cifrado de información, Control de Accesos, entre otros.), servicios que deberán cumplir con los niveles de servicio establecidos para que de manera inmediata y en donde lo requiera el Instituto se continue con la operación. Estos servicios serán bajo demanda a petición expresa del instituto, así como los tiempos de entrega serán conforme al sitio y dependiendo del tipo de tecnología en una modalidad de alta disponibilidad (HA), así como los niveles de servicios requeridos tanto para la implementación, como la operación, incluyendo los temas de soporte y resolución de problemas e incidentes.

2. **Servicios de Seguridad – Verificación y Calidad**
   Consiste en los requerimientos necesarios para que los servicios de calidad de la Seguridad de la Información se continúen, como son, aseguramiento de aplicaciones, cumplimiento normativo, herramientas de seguridad, ciberinteligencia, protección de datos, protección de redes inalambricas, seguridad de dispositivos móviles y de escritorio, control de acceso a la red, aseguramiento de cuentas privilegiadas, gestión de dominios, administración de certificados digitales, así como los niveles de servicio requeridos en la operación, incluyendo el soporte y resolución de problemas e incidentes.

3. **Servicios del Centro de Operaciones de Seguridad (SOC)**
   El Instituto requiere que el proveedor del servicio cuente con un Centro de Operaciones de Seguridad (SOC), que se encuentre físicamente en las instalaciones del proveedor. El objetivo de este centro deberá de ser la continuidad de la gestión de la seguridad y responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad, la ejecución de actividades de revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, análisis forense, analisis de ciberamenazas avanzadas, auditoria de reglas de acceso, notificación de alertas y vulnerabilidades, así como el establecimiento de acciones de mejora sustentable, la gestión del centro de operaciones de seguridad, parches y actualizaciones de las firmas de las soluciones de seguridad, que opere 7x24x365. El SOC deberá acreditarse con presentación de la copia simple del certificado ISO/IEC27001:2013 e ISO/IEC20000-1:2018 vigentes a nombre del licitante.

ANEXOS
DIVISIÓN DE CONTRATOS

## Partida 2

1. **Análisis de Vulnerabilidades Estático**
   El instituto requiere la continuidad de servicios de análisis de vulnerabiliades estáticos (aseguramiento de aplicaciones) que permitan atender a la protección de vulnerabilidades nuevas o conocidas, que representen una riesgo, en lo que a seguridad de la información se refiere, en el desarrollo de aplicaciones en sus diferentes etapas de construcción.

2. **Análisis de Vulnerabilidades Dinámico**

   El instituto requiere la continuidad de servicios de análisis de vulnerabiliades dinámicos que permitan atender a la protección de vulnerabilidades nuevas o conocidas, que representen un riesgo, en lo que a seguridad de la información se refiere, en todos aquellos activos de infraestructura que dan soporte a las aplicaciones y sistemas informáticos.

3. **Servicios de Análisis Forense**

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

4. **Servicios de Pruebas de Penetración**

   El Instituto requiere la continuidad de un servicio que permita realizar un proceso sistemático para comprobar las vulnerabilidades de las aplicaciones y la infraestructura que la soportan, con el propósito de buscar huecos o fallas en la seguridad.

Los servicios objeto de esta contratación se adjudicarán por **partida** a un solo licitante, cuya proposición cumpla con la totalidad de los requisitos de cumplimiento obligatorio; y haya obtenido la mayor puntuación en la evaluación combinada de puntos o porcentajes conforme a lo siguiente:

Por la naturaleza técnica de los servicios del SASI 2022-2024, en el caso de las partidas 1 y 2, los licitantes únicamente podrán participar en una de las dos partidas, lo anterior para evitar conflicto de interés técnico en detrimento del IMSS.

En este sentido, se hace del conocimiento de los Licitantes que, derivado de la naturaleza de los servicios y por sus características técnicas, bajo ningún escenario se podrá adjudicar las partidas 1 y 2 a un mismo licitante al que se haya asignado una de las 2.

**6. Requerimientos del Servicio - Especificaciones Técnicas**

**Partida 1.**

## 6.1. Servicios de Seguridad – Continuidad Operativa

### 6.1.1. Servicios de Firewall

**Descripción del servicio**: El instituto requiere de la continuidad operativa del servicio que proporciona la seguridad y protección de control de acceso, filtrado y bloqueo contra ataques dirigidos a las aplicaciones e inspección sobre los paquetes a nivel de aplicación para identificar patrones de tráfico anómalo, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondientes, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo *stand alone* para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.



ANEXOS
DIVISIÓN DE CONTRATOS



2022 Año de Ricardo Flores Magón

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

    - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

    - Notificar sobre fallas relacionadas con el *hardware* de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*; Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales *web* u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispostivos firewall para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

### 6.1.2. Servicios de Prevención de Intrusos (IPS)

**Descripción del servicio**: El Instituto requiere de la continuidad operativa del servicio que brinda la protección perimetral basado en firmas y que identifica vulnerabilidades, para contener los intentos de obtener acceso a los recursos o servicios publicados en Internet o Intranet que pudieran afectar la operación de la organización, detectar accesos no autorizados y prevenir fugas de información, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware/software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente.

- Permitir únicamente el tráfico (interno y externo) definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

- Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*; Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales *web* u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispostivos IPS para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto

- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice A.

### 6.1.3. Servicios de Protección contra Ataques Denegación de Servicio (DDoS)

**Descripción del servicio**: El Instituto requiere la continuidad operativa del servicio que protege contra los ataques de denegación de servicio distribuido que se encuentre basado en firmas y volúmenes de conexión altos, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondientes, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware o software que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

    - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

    - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del software que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de software y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software; Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales *web* u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

    - Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

    - Incluir un servicio de auditoría de reglas de acceso en los diferentes dispostivos DDoS para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

    - Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

### 6.1.4. Servicios de Redes Privadas Virtuales (VPN)

**Descripción del servicio**. El Instituto requiere la continuidad operativa del servicio de interconexión a través de Internet que permita establecer la comunicación desde localidades remotas para la transferencia de información a través de un canal cifrado, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

- Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea requerido por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo independiente (*stand alone)* para la administración de los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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



ANEXOS
DIVISIÓN DE CONTRATOS

2022 Año de Ricardo Flores Magón

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

  - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del software que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispostivos VPN para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.5. Servicios de Filtrado de Contenido Web**

**Descripción del servicio**. El Instituto requiere la continuidad operativa del servicio de filtrado de contenido Web mediante políticas de acceso que permite controlar y filtrar la utilización del servicio de acceso a Internet, en función de roles y perfiles, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

- Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

  - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del software que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de

soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispostivos de Filtrado de Contenido Web para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.6. Servicios de Filtrado de Contenido de Correo (Antispam)**

**Descripción del servicio**. El Instituto requiere la continuidad operativa de un servicio para analizar correos electrónicos de entrada y salida con el objetivo de bloquear aquellos que sean clasificados como spam, malware, phishing y con contenido malicioso, entre otros, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Proteger el correo electrónico de entrada y salida, asi como la reputación del direccionamiento IP que se utiliza para generar esta comunicación en Internet, para lo cual deberá incluir, un servicio de protección a través de los activos de infraestructura existente asi como un mecanismo de sanitización en la nube de Internet que prevea una doble capa de verificación sobre correos anómalos o no deseados (spam), con virus o malware.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de

todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

  - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispostivos Antispam para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.7. Servicios de Firewall Especializado en Servicios Web (WAF)**

**Descripción del servicio**. El Instituto requiere la continuidad del servicio de protección, prevención y control de ataques para aplicativos web expuestos en Internet/Intranet, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

- Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

    - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

    - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del software que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispostivos WAF para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.8. Servicios de Firewall especializado en Base de Datos (DBF)**

**Descripción del servicio**. El Instituto requiere la continuidad operativa del servicio de protección a las instancias de bases de datos en tiempo real, así como el monitoreo del tráfico de base de datos con la finalidad de realizar la detección de ataques avanzados, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

- Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (Base de datos), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las zonas de servidores.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

    - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

    - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección

de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispostivos DBF para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

### 6.1.9. Servicios de Gestión Unificada de Amenazas (UTM)

**Descripción del servicio**. El Instituto requiere la continuidad operativa del servicio de protección perimetral especializada en control de acceso, prevención de intrusos, filtrado de contenido Web y VPN, para control de tráfico y detección de actividad anómala, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

    - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

    - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware*

y/o *software*. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispostivos UTM para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

### 6.1.10. Servicio de Correlación de Eventos

**Descripción del servicio**. El Instituto requiere de un servicio de seguridad que administre, analice, explote, emplee y aproveche las bitácoras de los dispositivos de seguridad con la finalidad de conocer exactamente qué pasa en distintos puntos de la red de forma centralizada y eliminar falsos positivos generados, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar activos de infraestructura nuevos de última generación y dedicados exclusivamente para las necesidades del Instituto.

- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).

- Integrar activos de infraestructura de propósito específico (*appliances* o servidores físicos) con capacidades de expansión bajo demanda conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación de los nuevos activos de infraestructura para correlación de eventos en la arquitectura de seguridad y comunicaciones.



ANEXOS
DIVISIÓN DE CONTRATOS
2022 Ricardo Flores Magón
Año de

- Ejecutar todas las tareas necesarias para la instalación del equipo en los Centro de Datos correspondientes, o en su caso, aquella otra localidad donde le sea requerido por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.

- Integrar cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo independiente (*stand alone)* para la administración de todos los dispositivos, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Asegurar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente.

- Permitir únicamente la correlación definida por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión via syslog con otras redes o nubes.

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

- Monitorear los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

- Notificar sobre fallas relacionadas con el *hardware* de los activos de infraestructura provisto a través del servicio.

- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el proveedor del servicio deberá presentar la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.

- Integrar el licenciamiento del *software* que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) que permitan identificar, entre otros: mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en software que permitan acceder a las mismas (*aplicaciones* cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos del Correlacionador de Eventos para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice A.

### 6.1.11. Servicio de Protección de Amenazas Persistentes Avanzadas (APT)

**Descripción del servicio**. El Instituto requiere la habilitación de un servicio que le permita tener la capacidad de protegerse de amenazas avanzadas que se encuentren activas en la organización y que hayan podido sobrepasar los controles de seguridad existentes, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar activos de infraestructura nuevos de última generación y dedicados exclusivamente para las necesidades del Instituto.

- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).

- Integrar activos de infraestructura de propósito específico (*appliances*) con capacidades de expansión bajo demanda, pudiendo ser estas últimas instancias virtuales, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación de los nuevos activos de infraestructura para Amenazas Persistentes Avanzadas en la arquitectura de seguridad y comunicaciones.

- Ejecutar las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la

correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware/software* que integran el servicio sin un control de cambios autorizado por este último.

- Integrar cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Asegurar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente.

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

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

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

- Monitorear los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

- Notificar sobre fallas relacionadas con el *hardware* de los activos de infraestructura provisto a través del servicio.

- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el proveedor del servicio deberá presentar la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.

- Integrar el licenciamiento del *software* que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) que permitan identificar, entre otros: mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones

cliente-servidor, portales *web* u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos del servicio de Amenazas Persistentes Avanzadas para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice A.

## 6.2. Servicios de Seguridad – verificación y calidad

El Instituto requiere continuar con la prestación de servicios bajo demanda durante la vigencia del contrato y que a través de este se definan, identifiquen, clasifiquen y prioricen las debilidades de las aplicaciones que proporcionan una evaluación de las amenazas previsibles, que permitan reaccionar de manera apropiada, así como robustecer la confidencialidad, integridad y disponibilidad de la información, atendiendo a las necesidades operativas del IMSS.

### 6.2.1. Servicios de Borrado Seguro de Información

**Descripción del servicio.** Se requiere dar continuidad a la solución de borrado seguro de información, para los dispositivos tales como computadoras personales, laptops, servidores, unidades de almacenamiento fijas, removibles, externos y cualquier otro que el Instituto determine, con el fin de evitar la pérdida y dispersión de información propiedad de este; lo anterior aplicará cuando sean retirados dichos dispositivos por motivos de conclusión de contrato, obsolescencia, falla, baja y/o reasignación, entre otros. Para tal efecto se requiere la renovación del derecho de uso y soporte técnico de los productos de *software* de borrado seguro, así como, la actualización de dicho licenciamiento, actualizaciones (*updates* y *upgrades*) que permitan garantizar la confidencialidad de la información propiedad del Instituto, cumpliendo con lo establecido en la legislación vigente y aplicable relacionada con los derechos de autor.

Los servicios proporcionados por el proveedor, así como las entregas de información requeridas en el presente documento, deberán apegarse a la normativa vigente aplicable para dichos servicios y soluciones, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Integrar todas aquellas renovaciones que sean necesarias durante la vigencia de los servicios.

- Garantizar que las herramientas de borrado seguro cuenten con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios del servicio correspondiente.

- Deberá permitir realizar borrados completos en medios de almacenamiento dispuestos en activos de infraestructura como: equipos de cómputo (de escritorio y portátil), equipos de propósito específico (*appliance*), servidores físicos o virtuales, derivado de la sustitución, migraciones o retiro por finalización del contrato.

- Deberá asegurar que los datos no puedan ser recuperados, basándose en al menos los siguientes estándares internacionales.

    - HMG Infosec Standard 5 (baseline and enhanced)
    - Opnavinst 5239.1A
    - Extended NIST 800-88
    - DoD 5220.22-M
    - ISO-IEC 15408
    - ECE y BSI/VSITR

- Borrado de Discos duros IDE/ATA, SCSI, SAS, USB, SATA, SSD, Fiber Channel y FireWire, de estado sólido y mecánicos de cualquier tamaño.

- Deberá brindar la destrucción local y/o remota en múltiples dispositivos de almacenamiento.

- Deberá posibilitar el desmontaje RAID (SCSI).

- Deberá permitir el borrado y detección de zonas bloqueadas / ocultas (DCO, HPA).

- Deberá generar certificados de borrado infalsificables que ofrezcan protección ante cualquier instancia legal, en donde se incluya el resultado del proceso de borrado, fecha, hora, los datos del equipo, el detalle del dispositivo de almacenamiento borrado.

- Deberá emitir una firma electrónica para la autenticación de la integridad del reporte de sanitización emitido por el *software* de borrado.

- La solución deberá ejecutarse sin importar de que sistema operativo se trate.

- El reporte que generé la solución deberá ser exportado a un medio de almacenamiento como USB o disco duro.

- El servicio de borrado seguro esta provisto mediante un proceso o flujo operativo, el cual deberá contemplar entre otros, los siguientes puntos:

    - Solicitud de borrado.
    - Identificación del medio de borrado.
    - Definición de fecha de borrado.
    - Flujos operativos para la autorización de borrado o destrucción.
    - Como referencia, se muestran los insumos a ser atendidos

| DISPOSITIVOS |
|---|
| **Derecho Uso de Licencias y Soporte Técnico** |
| PC y Laptops |
| Servidores |
| Máquinas Virtuales y Unidades Lógicas |
| Archivos, carpetas, bases de datos |
| Console Management |
| **Servicio de Soporte Técnico Especializado** |
| Disco Duro, PC, Laptops, Disco Duro Servidor y Disco Duro Storage |
| Borrado de Bases de Datos, LUN's y Contenedores |
| Borrado de Máquinas Virtuales |
| Degaussing Discos Duros, SSD y Cintas LTO |

- La continuidad del servicio deberá considerar que los usuarios puedan acceder a las consolas de administración de la solución para la gestión, administración, supervisión y operación, todo ello con el fin de habilitar las funcionalidades operativas para realizar el borrado seguro de manera descentralizada (en oficinas remotas).

**6.2.2. Servicio de Gestión de Dominios**

**Descripción del servicio**. Continuidad operativa del servicio que permita registrar ante las instancias certificadas por el NIC, los dominios que requiera el Instituto y su correcta gestión, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Registro – Llevar a cabo el seguimiento correspondiente ante las instancias certificadoras
  - Revisar y dar seguimiento a el nombre de domino acordado con el personal designado por el Instituto
  - Revisar que no se encuentre duplicado o usado por ningún tercero

- Alojamiento – Dar seguimiento al alojamiento de dicho dominio
  - Actualización de las directivas de seguridad.
  - Continuidad al mantenimiento requerido

El proveedor de servicios deberá continuar con la gestión y los pagos que correspondan derivados del registro, cambio de dominio o proveedor sin costo adicional para el Instituto.

**6.2.3. Servicio de Certificados Digitales SSL**

**Descripción del Servicio**. Se requiere la continuidad del servicio que permite contar con certificados SSL para la protección de las páginas web del Instituto, durante la vigencia del contrato, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Validación de dominios
- Cifrado SSL de al menos 256 bits
- No debe de ser auto firmado, sino emitido por una instancia certificadora válida (tercero confiable)
- El tiempo de emisión deberá cumplir con los niveles de servicios establecidos para hacerlo llegar al personal del Instituto vía correo electronico

- El proveedor deberá hacerse cargo de la gestión en cuanto a pagos de derecho y cualquier cargo derivado de contar con el o los certificados.
- Los certificados deberán ser al menos de los siguientes tipos:
    - Certificados SSL con validación de dominio (DV SSL)
        - Certificado para un solo dominio
        - Certificado para múltiples dominios (SAN)
        - Certificados comodines (wildcard)

**6.2.4. Servicios de Ciberinteligencia (Ciberseguridad)**

**Descripción del servicio**. El Instituto requiere de un servicio con inteligencia accionable que le permita actuar oportunamente para protegerse y minimizar amenazas o ataques informáticos detectados a través de campañas y operaciones identificadas, al mismo tiempo que pueda ordenar investigaciones de acuerdo a sus necesidades, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Detectar posible venta de información confidencial del Instituto en mercados negros.

- Dar seguimiento a grupos hacktivistas y del cibercrimen nacionales y extranjeros que puedan representar una amenaza para el Instituto.

- Poder infiltrarse en canales de IRC donde se perpetren y difundan campañas de ataques informáticos que puedan afectar al Instituto.

- Monitorear foros y comunidades tanto de redes abiertas como de la Red Onion/TOR donde se perpetren y difundan campañas de ataques informáticos que pudieran representar un riesgo para el Instituto.

- Poder monitorear las noticias tanto nacionales como extranjeras tanto en la red abierta como en la Deep Web para la colección de inteligencia táctica, que permita al Instituto tomar acciones preventivas adicionales para la protección de infraestructura susceptible de un ataque informático.

- Colectar, a través de un cuestionario especializado, los elementos que provean la información necesaria para realizar el análisis de la situación global del Instituto, así como generar los perfiles de investigación a ser utilizados para los servicios permanentes.

- A través de un cuestionario en esta etapa se deberá recopilar la siguiente información:

    - Páginas publicadas.
    - Historial de amenazas de seguridad experimentadas por el Instituto.
    - Sistemas críticos consultados por usuarios externos.
    - Lista de activos críticos y su atracción o valor para el ciber-crimen.
    - Contactos para la elaboración de la matriz de escalación.
    - Datos para la elaboración de la declaración de trabajo (SOW por sus siglas en inglés).

- Realizar un análisis de la situación global del instituto, una vez teniendo el contexto de su entorno e identificando el tipo de exposición y amenazas que podrían impactarle de acuerdo al acontecer local y las amenazas globales del sector en el que se desenvuelve.

- Generación de perfiles de investigación con la información recabada. Dicho perfil de investigación deberá ser utilizado durante la vigilancia de Ciberinteligencia, el cual incluye lo siguiente:

  - Perfiles virtuales a emplear.
  - Definición de fuentes asociadas a los perfiles virtuales utilizados en el monitoreo.

- Determinar los umbrales para los eventos que dispararán las alertas que se deberán de notificar hacia la matriz de notificación definida en conjunto con el Instituto para los servicios como "Vigilancia Permanente de Ciberinteligencia".

- Mantener supervisión de los correos/sitios de phishing y direcciones IP dudosas que le comparta el instituto con el fin de realizar un análisis de los mismos. De manera adicional deberá realizar vigilancia en el ciberespacio las 24 horas del día los 365 días del año, sobre redes sociales, Darknet, buscadores de internet de las cosas, entre otras fuentes, para ello se deberá colectar inteligencia empleando técnicas de OSINT (Open Source Intelligence) como líneas de tiempo y mapas de conexiones, Virtual HUMINT donde se emplean la infiltración de perfiles virtuales.

- Identificar campañas para ataques específicos, venta de información, infraestructura vulnerable expuesta a través de internet, relaciones entre perfiles, grupos privados de facebook, entre otros.

- Realizar esta evaluación en cualquiera de los siguientes casos:

  - Durante la vigilancia de Ciberinteligencia, al encontrarse algún hallazgo que represente realmente una amenaza para el Instituto, se deberá realizar una notificación inicial con la finalidad de que el Instituto pueda tomar las líneas de acción necesarias para mitigar la amenaza descubierta.
  - Cuando se solicite el análisis de sitios dedicados al phishing, correos que contengan phishing o direcciones IP.
  - Durante la elaboración del análisis del comportamiento de los grupos hacktivistas.
  - Durante el análisis de las direcciones IP, producto de ataques de denegación de servicios que haya experimentado el Instituto.

- Realizar un análisis correlacionando toda la información recolectada por las herramientas y la situación general alrededor del evento, a partir de este análisis deberá emitir un dictamen hacia el instituto con inteligencia accionable, táctica u operativa según corresponda, en un plazo no mayor a 24 horas después de la detección de cualquiera de los siguientes eventos:

  - Declaración de posibles ataques de denegación de servicio por parte de grupos hacktivistas o del cibercrimen.
  - Defacements.
  - Fuga de información confidencial del Instituto hacia sitios públicos.
  - Malware dirigido.
  - Phishing detectado en parking domains.
  - Indicios de amenazas o ataques informáticos sobre el Instituto.

- Existencia de campañas (conjunto de acciones para perpetrar un ataque informático) en contra del Instituto.
- Venta o publicación de información sensible del Instituto en la Darknet.
- Publicación de información confidencial de personal del Instituto como usuarios y contraseñas.
- Nuevos esquemas de fraude detectados en otros organismos del sector.

- Para cualquier otro tipo de evento distinto a los listados solo deberá realizarse la notificación inicial.

- Deberá generarse el proceso de inteligencia accionable en cualquiera de los siguientes casos:
  - Cuando se detecte que un ataque ya sucedió y tuvo un impacto en el Instituto, para lo cual se emitirán recomendaciones hacia el Instituto.
  - En los casos donde se realice el análisis a petición del Instituto de sitios o correos relacionados con phishing así como direcciones IP, se deberá generar a partir de los hallazgos identificados inteligencia accionable donde deberán incluirse detalles sobre los sitios, direcciones IP, artefactos maliciosos, entre otros, al igual que sobre los reportes generados como parte de los servicios.

- Realizar el análisis de hasta 50 direcciones IP que el Instituto considere dudosas por mes, con el objetivo de analizarlas en búsqueda de información relacionada con ataques, además de determinar si éstas han realizado intrusiones a otros organismos de similares características a las del Instituto, si forman parte de una botnet, han sufrido un defacement, o bien forman parte de alguna campaña en particular.

- Analizar el comportamiento del hacktivismo en México y su relación con otros grupos, incluyendo el detalle de las operaciones del mes en curso, sus objetivos y el impacto de las mismas, así como recomendaciones para protegerse ante las nuevas operaciones esperadas.

- Analizar hasta 3 correos electrónicos o sitios al mes, con los cuales se realizarán entre otras las siguientes acciones:

  - Identificación de los encabezados y análisis del malware en el contenido.
  - Extracción de datos como dominios y direcciones IP, mismas que deberán ser analizadas en una plataforma de "Inteligencia sobre Amenazas" para determinar el riesgo que representa el Phishing para el Instituto.

**6.2.5. Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos Móviles.**

**Descripción del servicio**. El Instituto requiere un servicio de protección en redes inalámbricas específicas que permitan colocar controles que garanticen y protejan la información producida internamente y recibida a través de los recursos de redes inalámbricas (WLAN), contra ataques generales que buscan aprovechar esta modalidad para infiltrarse en la red de comunicaciones del Instituto, así mismo se requiere un servicio de protección de dispositivos móviles, que prevenga el robo o sustracción de información considerando para lo anterior, la administración de políticas y el cumplimiento de operación en los dispositivos móviles, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Garantizar que las herramientas propuestas para el servicio cuenten con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios con el que cuente el servicio correspondiente.

- Integrar el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.

- Proteger contra ataques informáticos comunes a la red inalámbrica (WLAN).

- Actualizar y mejorar los procesos que permitan la autenticación de usuarios internos.

- Cifrado TKIP y AES basado en *hardware*.

- Tener la funcionalidad de WIPS en tiempo real (prevención de intrusiones inalámbricas).

- Integrado en un tercer radio de banda doble específico (sin afectar el rendimiento del punto de acceso).

- Permitir aplicar políticas de control sobre las aplicaciones que los dispositivos

- Permitir la instalación de aplicaciones y ejecutar actualizaciones en múltiples dispositivos a la vez de manera remota y controlando el tipo de conexión y la fecha de ejecución
- Permitir realizar modificaciones de cambio de contraseña de bloqueo, y también se puede configurar la longitud, el tipo de contraseña, si es alfanumérica o numérica, el número de intentos, entre otros.

- Permitir a los administradores del sistema mantener y controlar estos dispositivos de forma centralizada.

- Analizar los dispositivos para asegurarse de que cumplen con la política del Instituto.

- Recuperar toda la información sobre los dispositivos, incluidos los detalles del dispositivo, certificados, aplicaciones instaladas, entre otros.

- Regular el acceso a las cuentas Institucionales tales como cuentas de correo electrónico, Wi-Fi y VPN.

- Bloquear los dispositivos de forma remota para evitar robados o perdida de información.

- Deberá soportar la conexión desde dispositivos móviles y de escritorio a través de un cliente de acceso remoto. Dicho cliente debe soportar al menos las siguientes plataformas operativas: MAC OS X, iOS, Android, Windows desde v7.

- Alarmas.

### 6.2.6. Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA).

**Descripción del Servicio**. El Instituto requiere un servicio de control de acceso para usuarios privilegiados con la intención de entregar en los servidores las funcionalidades de control y monitoreo de las cuentas de usuarios privilegiados existentes en cada uno de ellos, así como un mecanismo de Autenticación, Autorización y Contabilización (AAA por sus siglas en inglés, Authentication, Authorization and Accounting), por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Contar con una solución tecnológica que controle de manera granular el acceso a los activos de infraestructura que soportan las aplicaciones, a través de la administración del ciclo de vida de identidades.

- Integrar procesos que identifique los roles y perfiles de cada usuario por aplicación, así como la trazabilidad de los accesos realizados.

- Considerar, de manera enunciativa más no limitativa, las siguientes plataformas operativas:
  - Microsoft Windows
  - Unix
  - Linux

- Revisar y validar en conjunto con el Instituto los requerimientos de protección de las claves privilegiadas en los servidores en que se vaya a habilitar para el servicio.

- Implementar los agentes propiciados por la solución en sistemas operativos soportados por los fabricantes correspondientes.

- El proveedor deberá llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona de los Centro de Datos donde le sea solicitado.

- El proveedor deberá acordar con el personal del Gobierno de Contrato las ventanas de mantenimiento necesarias según el tiempo de implementación del que se trate.

- El proveedor deberá integrar el dispositivo hacia la consola de administración de la solución, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.

- Servicios de autenticación, autorización y registro (AAA) para habilitar el control de acceso e identidad hacia la red del Instituto.

- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).

- Uso de RADIUS la autenticación de acceso a la red.

- Uso de TACACS+ para la autenticación para accesos administrativos a la infraestructura del Centro de Datos.

- Deberá ser capaz de soportar la administración de al menos 5,000 dispositivos de red.

- Administración centralizada para políticas de acceso de gestión y VPN.
- Capacidad de generar políticas basadas en reglas y atributos.
- Capacidad de generación de políticas con asignación de VLANs.
- Integración con bases de datos externas tales como Active Directory y LDAP.
- Capacidad de integrarse a un dominio de Directorio Activo.
- Integración con soluciones de contraseñar únicas.
- Integración con los dispositivos de red para asegurar la aplicación de políticas de seguridad basadas en identidad.
- Uso de los siguientes protocolos de autenticación:
  - CHAP/MSCHAP
  - PAP
  - PEAP
  - EAP-TLS
  - MS-CHAP
  - EAP-MD5
  -
- Generación de políticas de restricciones por dispositivo y hora del día.
- Uso de listas de acceso descargables.
- Capacidad de operar en esquemas conglomerados (clúster) con más de 3 dispositivos operando como un solo sistema.
- Capacidad de operar en esquemas de procesamiento físico (appliance) o virtualizados
- Interface de administración gráfica basada en web
- Interface de programación para actualizar, crear, leer y borrar operaciones de dispositivos, terminales y usuarios de la base de datos interna.
- Funciones de reporteo y auditoría
- Capacidades de monitoreo y diagnóstico de problemas
- Administración de mensajes de eventos (logs) exportables.

**6.2.7. Servicio de Antivirus**

**Descripción del servicio.** El proveedor deberá proporcionar el licenciamiento, instalación, habilitación, configuración, puesta a punto, gestión, monitoreo, soporte y mantenimiento de una solución, que pueda poner en riesgo su funcionalidad, comprometiendo la seguridad en la actividad de los usuarios.

La protección de antivirus deberá realizarse a través de un agente, el cual deberá ser distribuido a los activos de infraestructura que el Instituto solicité, siendo responsabilidad del proveedor garantizar la entrega de dicho agente a los activos de infraestructura indicados por el Instituto, la distribución y administración puede ejecutarse onpremise o nube.

El proveedor deberá considerar que las actividades de remediación en infecciones de virus, serán su responsabilidad, por lo que deberá brindar el apoyo correspondiente a través de la explotación de las funcionalidades de la solución del antivirus propuesta como parte del presente servicio. El proveedor deberá notificar al personal que Instituto designe sobre los hallazgos de actividad sospechosa vía correo electrónico, u otro mecanismo que ambas partes determinen. El proveedor deberá atender los incidentes de *malware* que puedan presentarse; conforme se determine en los Acuerdos de Nivel de Servicio, o en su caso, a los Acuerdos de Nivel Operativos.

Cuando la necesidad de instalación del Instituto sea de más de 200 agentes, el proveedor, en conjunto con el Instituto, deberán definir una estrategia que permita el despliegue del agente de Antivirus, así como adecuar la estrategia de entrega de actualizaciones de Antivirus en cada uno de los activos de infraestructura solicitados, sin afectar la operación del Instituto, considerando que dichos activos y consolas de administración se encontrarán distribuidos en las diferentes localidades del Instituto.

El proveedor deberá configurar en la solución de Antivirus propuesta, las políticas base de seguridad definidas en conjunto con el Instituto, como parte de las reglas que regirá el presente servicio, para los activos de infraestructura a los cuales les sea provisto, la cual deberá ser desplegada a los mismos a través de la consola de administración de la solución. A su vez, el proveedor deberá realizar la puesta a punto de las políticas definidas en la solución de antivirus propuesta, con fundamento en el monitoreo continuo de la misma y los requerimientos del Instituto.

El proveedor deberá definir una estrategia en conjunto con el Instituto que permita el despliegue para la entrega de actualizaciones de Antivirus en cada uno de los activos de infraestructura sin afectar las operaciones de los servicios internos, los cuales se encuentran distribuidos en las diferentes localidades de la CDMX. Será responsabilidad del proveedor mantener actualizados en todo momento los activos de infraestructura con la última versión o actualización de antivirus liberada por el fabricante.

El proveedor, en conjunto con el Instituto, definirá la cantidad de activos de infraestructura que constituirá la línea base para el primer año de prestación del servicio. Posteriormente, un mes antes de cumplir cada año de servicio se realizará una redefinición de la línea base para la prestación del servicio del próximo año.

El proveedor deberá entregar al personal del Instituto la última versión del agente de antivirus, para que este sea integrado dentro de la imagen de software de los Puestos de Servicio.

Como parte de la operación del presente servicio, el proveedor deberá:

- Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Antivirus.
- Monitorear el cumplimiento de las políticas de uso de información implantadas en la solución.

- Notificar sobre las actividades sospechosas relacionadas con la infección de activos de infraestructura.
- Notificar sobre todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la Solución de Antivirus, efectuando la contención de las mismas a través de la solución propuesta.
- Resolver las solicitudes de soporte técnico especializado, a fin de evitar y prevenir infecciones en los activos de infraestructura donde se encuentre instalada la solución de Antivirus.
- Recolectar e integrar, al menos la información de eventos de seguridad o logs generada por la solución de Antivirus, hacia la solución de correlación de eventos, cuyo detalle de información a integrar será definido entre el Instituto y el proveedor.
- Desarrollar la afinación de la solución con base en el resultado del monitoreo continuo, además de gestionar las reglas antivirus en los activos de infraestructura, con base en las necesidades del Instituto y en el resultado del monitoreo día a día.

### 6.2.8. Servicios de Prevención de Pérdida de Información

**Descripción del servicio.** El Instituto requiere una solución que permita detectar y evitar la fuga y/o pérdida de información sensible en los activos de infraestructura del IMSS instalados en los Centros de Datos, misma que debe estar integrada a los activos de infraestructura, servicio de correo electrónico externo, correo electrónico interno, navegación web y portales de colaboración, para una completa visualización y prevención en distintas capas de seguridad.

Dicho módulo debe tener la capacidad de generar políticas a través de palabras clave o expresiones regulares con la información sensible, bloqueando su transmisión a través de diversos canales de comunicación.

El servicio deberá enfocarse en prevenir fuga de información sensible desde los puestos de servicio.

El proveedor deberá configurar en la solución propuesta las políticas base de seguridad definidas en conjunto con el Instituto, para los activos de infraestructura, desarrollando los perfiles correspondientes.

Dichas políticas deberán ser desplegadas a través de la consola de administración de la solución, y el proveedor deberá realizar la puesta a punto de las mismas, con fundamento en su monitoreo continuo y los requerimientos del Instituto, para lo cual, el Instituto requiere que se tomen en consideración, como mínimo, las siguientes premisas:

- Tipos de documentos.
  Se refiere a las formas en las cuales se pueden estructurar los activos de información que son relevantes para los procesos del Instituto: reportes, estudios, oficios, correspondencia, acuerdos, directivas, planes estratégicos, contratos, convenios, anotaciones, memorandos, estadísticas, procedimientos, políticas, reglamentos, informes, solicitudes, encuestas, históricos, entre otros.

- Medios de almacenamiento de la información.
  Se refiere a los distintos medios en los cuales pueden resguardarse los activos de información para su posterior manipulación

El proveedor deberá asegurar que las funcionalidades de la Solución de Prevención de Pérdida de Información deberán cumplirse aun cuando el activo de infraestructura no se encuentre firmado a ningún Directorio Activo, o bien, a la red del Instituto.

Como parte de la operación del servicio, el proveedor deberá:

- Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Prevención de Pérdida de Información.
- Monitorear el cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificar al Instituto sobre actividades sospechosas relacionadas con la violación de las políticas sobre fuga de información configuradas en los activos de infraestructura.
- Efectuar la contención de actividades sospechosas.
- Atender a las solicitudes de soporte técnico especializado, a fin de evitar fugas de información en los equipos en los que se encuentre habilitada la solución.
- Recolectar e integrar, al menos la información de eventos de seguridad o logs generada por la solución de Prevención de Pérdida de Información, hacia la solución de correlación de eventos, cuyo detalle de la información a integrar será definido entre el Instituto y el proveedor.
- Administrar los elementos tecnológicos a través de procesos de gestión de cambios, configuraciones y versiones de acuerdo con los requerimientos del Instituto.

La solución propuesta por el proveedor deberá contar con las siguientes funcionalidades:

- Presente un log de auditoría de todas las actividades de los usuarios.
- Proporcione reportes predefinidos y personalizados que puedan ser programados o de una sola vez.
- Proporcione un mecanismo de alertas y notificaciones.
- Tecnología de Detección.
    - Capacidad para extraer textos de diferentes tipos de documentos para ejecutar escaneos de contenido.
    - Capacidad de realizar detecciones basadas en palabras (keywords) personalizadas o frases (key phrases) personalizadas, con la habilidad de poner diferentes palabras en una sola regla de detección.
- Debe de ser capaz de ejecutar escaneos de contenido en diversos canales de información (Correo, https/http, ftp, entre otros)

**6.2.9. Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)**

**Descripción del servicio.** Garantizar la continuidad operativa del Sistema de Gestión de Seguridad de la Información (SGSI), que deberá estar basado en el estándar ISO/IEC 27001:2013, mediante el cual se emitirán las directivas en materia de seguridad de la información a las áreas de TI y a los terceros que soportan la operación de TI, mismo que deberá considerar las actualizaciones que correspondan.

El proveedor del servicio deberá garantizar la continuidad operativa de este servicio y deberá cumplir con al menos las siguientes funcionalidades operativas:

**Planear**

- Capacitación de seguimiento – Curso "Inducción a la norma ISO/IEC 27001:2013 o vigente, que permita:

  - Conocer la estructura de la norma ISO/IEC27001:2013
  - Interpretar los requisitos solicitados para el cumplimiento de la norma
  - Conocer las etapas para la implementación de un SGSI
  - Se deberán considerar al menos 8 participantes, con un tiempo mínimo de 8 horas y máximo de 40 horas.

- Seguimiento y actualización en la aplicación de las directivas en materia de seguridad.
  Manual de políticas de seguridad de la información, que deberá apegarse a lo siguiente:
  - Dominios que establece la norma ISO/IEC 27001:2013
  - Procesos de seguridad aplicables en la normativa vigente.
  - Enfocarse a las áreas de TI y a los terceros que proveen servicios de TI al Instituto, considerando como alcance el catálogo de infraestructuras críticas del Instituto (al menos 20 directivas).

- Identificación y evaluación de activos (relacionado al catálogo de infraestructuras críticas) del proceso involucrado en el Sistema de Gestión de Seguridad de la Información.
  La metodología deberá considerar los siguientes temas:
  - Identificación de los activos del proceso.
  - Valoración de los activos del proceso.
  - Identificación de requerimientos de seguridad.
  - Identificación de los controles de seguridad existentes.

- Generación de la declaración de aplicabilidad. (SoA: Statement of Applicability).

  La metodología deberá considerar los siguientes temas:
  - Identificación y aplicabilidad de los requerimientos internos y externos
  - Selección de los objetivos de control y controles para el tratamiento de los riesgos
  - Verificación de requerimientos contractuales y legales
  - Identificación de los requerimientos internos y externos
  - Validación de aplicabilidad de los requerimientos
  - Formato de Autorización para implantar y operar el Sistema de Gestión de Seguridad de la Información
  - Preparación de la declaración de aplicabilidad
  - Documentar los objetivos de control y los controles elegidos y la justificación de su elección
  - Documentar los controles actualmente implementados
  - Documentar la exclusión de controles y la justificación de su exclusión

- Operación el Sistema de Gestión de Seguridad de la Información
  - Análisis de Riesgos de Seguridad de la Información
  - Análisis de riesgo con base en lo definido en el servicio de gestión de riesgos de seguridad
  - Generación de la actualización del plan de tratamiento de riesgos
    La metodología deberá considerar los siguientes temas:
  - Identificación de las acciones a realizar por parte de la institución y su administración
  - Identificación de los recursos necesarios y prioridades

- Identificación de las responsabilidades para administrar los riesgos de seguridad de la información

- Aplicación del seguimiento al plan de tratamiento de riesgos.
  La metodología deberá considerar los siguientes temas:
  - Asignación de los roles y responsabilidades en el seguimiento de los controles relativos a personas, procesos y tecnología involucrados en la mitigación de los riesgos.
  - Actualización de documentación, alineada a los requisitos establecidos en la normativa vigente

- Detalle y actualización de políticas y procedimientos de seguridad existentes

- Definición del proceso de reporte y atención de incidentes de seguridad

- Propuestas de implementación de los controles seleccionados.
  La metodología deberá considerar los siguientes temas:
  - Control de accesos
  - Monitoreo de cuentas
  - Definición del proceso de Continuidad del negocio
  - Implantación de los Roles y responsabilidades definidas para el Sistema de Gestión de Seguridad de la Información
  - Controles de seguridad en la infraestructura tecnológica de acuerdo con lo definido en el alcance.

- Administración del cambio cultural.
  La metodología deberá considerar los siguientes temas:
  - Actualización del Programa de concientización con usuarios y operadores del Sistema de Gestión de Seguridad de la Información
  - Seguimiento y apoyo a las necesidades de capacitación para el personal que administra el Sistema de Gestión de Seguridad de la Información y seguridad de la información
  - Manual de Gestión de Seguridad de la Información.
    Se deberá documentar un manual que contenga las referencias generadas en esta fase para dar trazabilidad al de las cláusulas de la norma.

- Monitorear y Revisar el Sistema de Gestión de Seguridad de la Información
  Revisiones gerenciales.
  La metodología deberá considerar los siguientes temas:
  - Los dueños del proceso deberán hacer una revisión y actualización al Sistema de Gestión de Seguridad de la Información con la finalidad de verificar que los objetivos del Sistema de Gestión de Seguridad de la Información están alineados a los objetivos de negocio en materia de seguridad de la información y que garantizan el adecuado manejo de los riesgos existentes.
  - El proveedor deberá actualizar el procedimiento de revisiones gerenciales.
  - El proveedor actualizará los formatos requeridos para llevar a cabo las revisiones gerenciales

- Auditorías internas.
  La metodología deberá considerar lo siguiente:

- Seguimiento y apoyo en la generación del plan de auditorías internas a las áreas de TI y a los terceros que proveen servicios de TI al Instituto.
- Actualización o en su caso definición de los formatos requeridos para llevar a cabo las auditorías
- Aplicación de una auditoría interna al Sistema de Gestión de Seguridad de la Información para verificar el cumplimiento con el estándar ISO/IEC 27001:2013 o vigente y a los procesos establecidos en la normativa vigente aplicable.

- Actualización del Sistema de Gestión de Seguridad de la Información
  Implementación de mejoras
  Deberá considerar los siguientes temas:
  - Priorización de las acciones correctivas y no conformidades identificadas en las revisiones gerenciales, revisiones independientes, auditorías internas y revisiones técnicas
  - Identificación de los responsables de llevar a cabo las mejoras.
  - El Instituto definirá las fechas compromiso para la terminación de las mejoras, únicamente para seguimiento interno.

- Acciones correctivas y no conformidades.
  Deberá considerar lo siguiente:
  - Apoyo en la definición y seguimiento del procedimiento para realizar acciones correctivas y no conformidades derivadas de las auditorias.
  - Actualización del formato para llenado de acciones correctivas y no conformidades.
  - Coordinación de la ejecución de las acciones correctivas ya definidas y en su caso las no conformidades que se identifiquen.

- Comunicar los resultados de las acciones tomadas.
  Se deberá considerar lo siguiente:
  - Apoyo en la programación de reuniones de seguimiento al Sistema de Gestión de Seguridad de la Información para dar a conocer el alcance de las acciones correctivas y no conformidades realizadas y verificar su apego a los requerimientos de los dueños de la información y a los involucrados en los procesos del Instituto.

### 6.2.10. Servicios Continuidad de Gestión del Cambio en Seguridad de la Información

**Descripción del servicio.** El Instituto requiere de la integración de un programa de gestión del cambio para la protección de la información, alineado a los requerimientos del estándar ISO/IEC27001:2013, siguiendo una estrategia cultural.

Este servicio deberá contar con un plan de transferencia de conocimiento al personal del Instituto en los principales temas de seguridad de la información considerando al menos los siguientes rubros:

- Regulación vigente en materia de seguridad de la información.
- Políticas de seguridad del Instituto.
- Procesos de seguridad del Instituto.
- Controles de seguridad implementados en el Instituto.

El servicio se describe en las etapas que a continuación se indican:

Etapa 1. Definición de la estrategia de gestión del cambio

- Contextualización del Instituto. El proveedor deberá tener el contexto cultural del Instituto en materia de seguridad de la información
- Diagnóstico del estado actual. El proveedor deberá llevar a cabo un diagnóstico del nivel de conocimiento en materia de seguridad de la información que presente la brecha entre la situación actual y la situación requerida por el Instituto
- Preparación de la estrategia. El proveedor, con base en los resultados obtenidos en el diagnóstico, deberá proponer una estrategia de gestión del cambio en seguridad de la información con el fin de hacer una adecuada transferencia del conocimiento.

Etapa 2. Diseño del programa de gestión del cambio

- Preparación del programa. El proveedor deberá generar un plan de trabajo detallado con los temas que forman parte de la transferencia del conocimiento, el número de personal involucrado y las fechas en las cuales se llevará a cabo.
- Preparación de contenidos. El proveedor deberá desarrollar los materiales en formato Power Point, u otros que el Instituto defina, que serán utilizados para la transferencia del conocimiento en seguridad de la información.
- Generación del modelo de evaluación. El proveedor deberá presentar un modelo de evaluación con el fin de identificar el grado de efectividad de la transferencia de conocimiento de seguridad de la información.
- Preparación del grupo de train traineers. El proveedor deberá identificar y preparar a un grupo de 5 trainees con el fin de que puedan replicar la transferencia del conocimiento a otras áreas sustantivas dentro del Instituto.

Etapa 3. Comunicación del programa de gestión del cambio

- Despliegue de la transferencia. El proveedor deberá llevar a cabo el despliegue de la transferencia del conocimiento al personal de TI del Instituto y de las áreas sustantivas definidas por este dentro de la Ciudad de México.

Etapa 4. Medición del programa de gestión del cambio

- Aplicación de evaluaciones. El proveedor habilitará una herramienta tecnológica con el fin de aplicar evaluaciones en línea a los participantes de la transferencia del conocimiento.
- Análisis de datos obtenidos. El proveedor deberá revisar la información obtenida con el fin de organizar los resultados obtenidos.
- Presentación de resultados generales. El proveedor deberá llevar a cabo una presentación ejecutiva con los resultados obtenidos al personal de TI del Instituto.

**Partida 2**

### 6.2.11. Servicios de Análisis de Vulnerabilidades Dinámico

**Descripción del servicio**. El Instituto requiere la continuidad operativa de un servicio que permita ejecutar análisis técnicos especializados sobre los activos de infraestructura de procesamiento, redes, sistemas y aplicaciones, con la finalidad de identificar vulnerabilidades nuevas o conocidas, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Integrar las tareas necesarias para la ejecución de los análisis de vulnerabilidades en los centros de datos que el instituto indique, o en su caso, en aquellas otras localidades donde le sea requerido.

- Dar seguimiento a los reportes a través de las herramientas con las que se cuentan, que permiten complementar los análisis de vulnerabilidades llevados a cabo.

- Renovación del licenciamiento del *software* que permite continuar con los servicios y activos de infraestructura que correspondan.

- Garantizar que las herramientas de análisis de vulnerabilidades cuenten con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios con el que cuenta el servicio.

- Identificar los servicios a analizar, incluyendo el número de equipos involucrados y la versión de las plataformas de los sistemas.

- Identificación de vulnerabilidades documentadas en organismos internacionales como el CVE (Common Vulnerability Exposures).

- Identificación de configuraciones por omisión.

- Capacidad para determinar el grado de vulnerabilidad ante técnicas de ataque como:
  - SQL injection
  - Cross Site Scripting
  - Cross Site Request Forgery
  - Sensitive Data Exposure
  - Security Misconfiguration
  - Broken Authentication and Session Management

- Elaborar un reporte ejecutivo y técnico, por cada requerimiento atendido, en el que se describan los detalles de los riesgos asociados a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP llamada "OWASP Risk Rating Methodology", detallando recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.

- Integrar un proceso y/o procedimiento para la continuidad de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada.

- El proveedor de servicios deberá integrar el mecanismo operativo necesario para llevar a cabo el proceso de remediación conforme las vulnerabilidades reportadas, contemplando personal especializado para las plataformas operativas y herramientas en *software* descubiertas.

### 6.2.12. Servicios de Análisis de Vulnerabilidades Estático

**Descripción del servicio.** El Instituto requiere identificar el nivel inicial de madurez de las prácticas de seguridad en el *software* con las que cuenta el Instituto, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Implementar una solución tecnológica que permita realizar pruebas dinámicas y estáticas de una manera centralizada y con soporte al menos a los siguientes lenguajes de programación: HTML, Java, .Net, C#, PHP.

- Integrar el licenciamiento del *software* que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.

- Garantizar que las herramientas propuestas para el servicio cuenten con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios con el que cuente el servicio correspondiente.

- Integrar un proceso de evaluación de las prácticas existentes de seguridad de *software* en el Instituto.

- Construir un programa de evaluación de seguridad de *software* con iteraciones definidas en conjunto con el Instituto.

- Actualizar y crear procesos en las diferentes etapas del ciclo de vida de desarrollo de *software* para asegurar el mismo.

- Ayudar en el cumplimiento del *software* basado en estándares y/o marcos normativos previamente definidos en conjunto con el Instituto.

- Identificar el nivel inicial de madurez de las prácticas de seguridad en el *software* con las que cuenta el Instituto.

- Identificar y entender el entorno del Instituto, personal relacionado, normatividad y tecnologías que cubran el alcance de la entrega del servicio para identificar el modelo de operación, flujos de interacción, entre otros, de las diferentes entidades que deben ser incluidas en el proceso.

- Integrar las mejores prácticas de seguridad en el *software* mencionadas en el modelo de madurez propuesto y alineado a OpenSAMM.

- Realizará la transferencia de las prácticas de seguridad en el *software* implementadas al personal que el Instituto designe para dicho propósito.

- Operar el modelo de madurez establecido, pudiendo certificar en 3 diferentes etapas el nivel de cumplimento el *software* evaluado, las cuales podrán ser:
  - Al inicio del desarrollo de una aplicativo.

- Durante el desarrollo de un aplicativo.
- Posterior al desarrollo de un aplicativo.

- Preservar la integridad y confidencialidad de la información recibida durante la ejecución de las pruebas dinámicas y/o estáticas correspondientes (cadena de custodia).

- Elaborar un reporte ejecutivo y técnico, por cada requerimiento atendido, donde se describa los detalles de los riesgos asociados a cada hallazgo o vulnerabilidad identificada, detallando recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.

**6.2.13. Servicios de Pruebas de Penetración**

**Descripción del servicio**. El Instituto requiere la continuidad de un servicio que permita realizar un proceso sistemático para comprobar las vulnerabilidades de las aplicaciones y la infraestructura que la soportan, con el propósito de buscar huecos o fallas en la seguridad, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Integrar todas las tareas necesarias para la ejecución de las pruebas de penetración en los centros de datos que el instituto indique, o en su caso, en aquellas otras localidades donde le sea requerido.

- Dar seguimiento a los servicios o activos de información que deberán ser analizados, incluyendo el número de equipos involucrados, y la versión de las plataformas de los sistemas analizados.

- Identificación de vulnerabilidades y malas configuraciones.

- Explotación de acceso a los sistemas mediante el aprovechamiento de los huecos de seguridad detectados y/o vulnerabilidades detectadas.

- Evaluación de vulnerabilidades de al menos los siguientes rubros:

  - Autenticación y Autorización
    - Intentos ilimitados de inicio de sesión
    - Insuficiente autenticación
    - Insuficiente autorización

  - Gestión de sesión
    - Predicción de sesión
    - Secuestro de sesión
    - Reproducir sesión
    - Expiración de sesión insuficiente

  - Inyección de código
    - Inyección comando de Sistema Operativo
    - Inyección SQL
    - Cross-site Scripting
    - Inyección LDAP

- Inyección HTML
- Parameters Tampering
- Cookie Poisoning
- Hidden Field Manipulation

- Criptografía
  - Fortaleza del algoritmo
  - Gestión de llaves
- Ataques Lógicos
  - Abuso de funcionalidades
  - Input Field Validation Checking
- Protección de Datos
  - Transporte
  - Almacenamiento
- Divulgación de Información
  - Indexado de directorio
  - Path Traversal
  - Manejo inseguro de errores
  - Comentarios HTML

- Realizar un reporte ejecutivo y técnico, por cada requerimiento atendido, en el que se describan los detalles de los riesgos asociados a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP llamada "OWASP Risk Rating Methodology", detallando recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.

- Integrar un proceso y/o procedimiento para la continuidad de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada.

- El proveedor de servicios deberá integrar el mecanismo operativo necesario para llevar a cabo el proceso de remediación conforme las vulnerabilidades reportadas, contemplando personal especializado para las plataformas operativas y herramientas en software descubiertas.

### 6.2.14. Servicios de Análisis Forense

**Descripción del servicio**. El Instituto requiere la continuidad de un servicio de análisis de incidentes de seguridad para determinar y documentar a través de la integración de registros o bitácoras las evidencias o indicios de eventos y su relación en el tiempo que identifiquen cuando ocurrió, que infraestructura, servicios tecnológicos o sistema de información fueron comprometidos, como fue realizado, y quien o que, estuvo relacionado con el incidente y el impacto del evento, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Integrar las tareas necesarias para la ejecución de los análisis forenses en los centros de datos que el instituto indique, o en su caso, en aquellas otras localidades donde le sea requerido.

- Continuar con la definición del objetivo parámetros y cuestionario que resulten de interés para la investigación solicitada.
- Dar continuidad y seguimiento a los casos solicitados, así como, el registro de los indicadores correspondientes.
- Preservar la integridad de la información recibida durante la ejecución del proceso de análisis forense (cadena de custodia).
- Participar en entrevistas con los principales involucrados con la finalidad de obtener el contexto necesario en las investigaciones digitales que deban realizarse.
- Obtener información de fuentes públicas en la red en caso de que estas pudieran llegar a ser relevantes para la investigación realizada.
- Realizar las evaluaciones de información en los equipos de cómputo, servidores físicos, servidores virtuales, dispositivos móviles, equipo de comunicaciones, entre otros, para la identificación de indicios de compromiso y su evidencia correspondiente.
- Llevar a cabo un proceso de recuperación de información que haya sido borrada previamente.
- Dar seguimiento a la herramienta colaborativa que tiene por objeto facilitar la visualización de hallazgos a los usuarios finales, así como generar reportes de hallazgos en caso de ser requerido.
- Elaborar un dictamen técnico, por cada requerimiento atendido, con la información identificada en el o los procesos de análisis forense, considerando la generación y firma de los documentos que expresen los resultados de la investigación en forma clara y concisa, de manera que puedan ser comprendidos por aquellos que no conocen o dominen el lenguaje técnico.

## 6.3. Servicios del Centro de Operaciones de Seguridad (SOC)

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

El servicio del Security Operatión Center (SOC) que soportará la operación y prestación del servicio requerido por el Instituto, deberá proporcionar un control continuo, una mayor eficiencia y oportunidad de mejora, para lo anterior el licitante deberá proporcionar servicios de tecnología de la información fiables en lo referente a la gestión de servicios de TI, mismos que deberá acreditar con las certificaciones ISO/IEC27001:2013 e ISO/IEC 20000-1:2018 vigentes y a nombre del Licitante.

El Licitante, deberá considerar que el servicio de SOC se refiere a las soluciones propuestas e implementadas hoy en día por el instituto, así mismo deberá considerar que la correlación de bitácoras se

deberá basar en un servicio de correlación de eventos e incidentes de seguridad en el que los casos de uso deberán ser ilimitados, así como las respuestas ante un incidente alineadas a tiempo de los niveles de servicio (SLA) establecidos para este servicio.

- Ubicarse dentro de territorio nacional, mismo que podrá acreditar con la copia simple a nombre del SOC del licitante del ISO/IEC27001:2013 e ISO/IEC20000-1:2018.

- Operación continua las 24 horas del día, los 7 días de la semana y durante los 365 días del año (7x24x365), esto último conforme la vigencia del contrato.

- Contar con personal para la atención del servicio en sitio y de forma remota, el cual deberá ser personal calificado con base en las credenciales requeridas para la administración y monitoreo de los componentes que integran la solución.

- Operación en un centro de datos alterno ubicado dentro de territorio nacional.

- Mantenimiento de las suscripciones a sitios y listas de empresas, fabricantes y medios especializados en seguridad de la información, que permitan alertar sobre nuevas vulnerabilidades.

- Infraestructura dedicada para la administración, operación y monitoreo de los componentes *hardware* y *software* que componen los servicios de seguridad.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones deberán ejecutarse cada 3 meses, desde el inicio de operaciones de los servicios y hasta 3 meses antes del término de estos.

- Realizar acciones correctivas y preventivas para asegurar la confidencialidad, integridad y disponibilidad de la información que se maneja en las diferentes soluciones se seguridad.

- Notificaciones y alertas personalizadas, en caso de desviaciones, anormalidades o brechas de seguridad, para cada una de las soluciones de seguridad.

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

- Analizar los eventos de seguridad y administración de bitácoras que se integran en los servicios de correlación de información, a fin de establecer acciones preventivas a través de modificaciones a las configuraciones de las soluciones de seguridad.

- Integrar un Equipo de Atención y Respuesta a Incidentes de Seguridad.

- Soporte y Atención a fallas a los componentes hardware y software que integran la solución, conforme los estipulado en los acuerdos de niveles de servicio

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

- Realizar mantenimiento preventivo y correctivo a las soluciones de seguridad habilitadas, así como a los activos de infraestructura que soportan cada servicio.

- Ejecutar procesos operativos para al menos los siguientes rubros:

  - Gestión de Riesgos
  - Gestión de Continuidad
  - Monitoreo y Detección
  - Gestión de Seguridad de la información
  - Administración de Dispositivos
  - Gestión de solicitudes de servicio
  - Administración de Cambios Operacionales
  - Administración de Configuraciones
  - Administración de Vulnerabilidades
  - Gestión de Incidentes
  - Gestión de Problemas

- Integración de una Mesa de servicio apegada a ITIL v4, la cual debe integrarse con la Mesa de Servicios Tecnológicos del Instituto, considerando todas las actividades de puesta a punto, desarrollo de piezas de software, configuraciones, entre otros, que permitan establecer la comunicación para la generación de requerimientos, cambios, incidentes, y otros procesos que determine el Instituto.

- El servicio de requerimientos, cambios, incidentes, entre otros, deberá permitir la generación de eventos (tickets), mediante los mecanismos que se establezcan en las mesas de trabajo correspondiente, que, de manera enunciativa más no limitativa, podrán ser:
  - Un número telefónico directo en las instalaciones del SOC.
  - Un número telefónico a diez dígitos.
  - Correo Electrónico
  - Portal Web

- El personal del proveedor del servicio, que atenderá las operaciones de los servicios de seguridad, deberá contar con experiencia probada en las áreas de tecnología y de seguridad de la información previamente mencionadas, para lo cual, deberá integrarse el currículo vitae de todo el personal que participe en el servicio, indicando al menos:
  - Experiencia profesional: bajo este rubro, se considerarán todos los puestos que cada integrante haya desempeñado, con fecha, nombre de los empleadores, nombre de los puestos que ha ejercido y el tipo de funciones bajo su responsabilidad, y deberá contar con experiencia comprobable al menos 3 años.

  - Experiencia en proyectos de su especialidad en Seguridad de la Información: bajo este rubro se citarán y describirán todos los proyectos en que se ha participado, y deberá contar con experiencia comprobable de al menos 3 años.

- Estudios: bajo este rubro se anotarán todos los estudios en materia de seguridad de la información, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica. Las certificaciones son de tecnología y/o de seguridad de tipo "vendor-neutral".

- Incluir la estructura del grupo de trabajo, indicando por cada perfil las responsabilidades y competencias

- El Instituto podrá solicitar la revisión de la infraestructura de seguridad por un tercero en cualquier momento, durante la vigencia del contrato, con la finalidad de dar certeza de la entrega del servicio.

- Seguimiento a la Base de Datos de la Gestión de la Configuración (CMDB por sus siglas en ingles) que contenga los detalles relevantes de cada elemento de configuración (CI) y de la relación entre ellos, incluyendo el equipo físico, software y la relación entre incidencias, problemas, cambios y otros datos del servicio de seguridad.

- Generar los reportes de Inteligencia de Negocio y Analítica de Información que permitan tener estadísticas del uso y desempeño de los servicios de seguridad, esto último con el objetivo de coadyuvar a la toma de decisión estratégica y operativa de los servicios, así como para determinar el plan de capacidad de cada tecnología implementada. Dichos reportes podrán considerar, de manera enunciativa más no limitativa, la siguiente información:

  - Estadísticas de uso de procesamiento por tecnología
  - Estadísticas de desempeño por tecnología (throughput)
  - Estadísticas de ataques informáticos bloqueados.
  - Estadísticas de comportamientos tipo esperado de uso por tecnología (líneas base)
  - Estadísticas de usuarios concurrentes por servicio.
  - Estadísticas de crecimiento diario, mensual y anual por cada servicio.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración de los servicios de seguridad, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Las consolas de administración provistas para los servicios de seguridad deberán permitir visualizar al menos:

  - Políticas: Control de Acceso
  - Configuraciones: Listas de Control de Acceso (Listas Blancas, Listas negras), Líneas base de seguridad.
  - Objetos: Usuarios, Grupos, Direcciones IP
  - Bitácoras.
  - Estadísticas en tiempo real: Desempeño, procesamiento, usuarios conectados, conexiones por segundo, ancho de banda utilizado.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para cada solución o servicio, donde se pueda consultar información sobre los casos de

soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso de los servicios de seguridad.

- Integrar un Tablero de Estadísticas de Servicios de Seguridad a través de un portal único de administración de los servicios de seguridad de forma independiente a las consolas de administración de los servicios de seguridad, así como de las herramientas de monitoreo que contenga información estratégicas sobre el uso de los servicios en tiempo real y de manera histórica, y que permita al Instituto tener el contexto general sobre el desempeño de las soluciones, su estado de salud, incidentes registrados, reportes de actividades sospechosas relevantes a nivel mundial, u otra información relevante que permita tomar decisiones sobre las condiciones de operación de los servicios, el licitante ganador debe incluir en su oferta económica los costos asociados al desarrollo para el cumplimiento de éste requerimiento.

- Permitir al personal que designe el administrador del contrato, generar reportes explotando todas las variables y funcionalidades de la herramienta de monitoreo, con la opción de parametrizar dichos reportes y consultarlos vía web.

### 6.5. Condiciones para la implementación de los servicios

El proveedor del servicio de SASI 2022-2024, será responsable de llevar a cabo la implementación de los servicios solicitados conforme a los plazos descritos en el presente documento, lo cual incluye las renovaciones o migraciones de tecnología que el cumplimiento de SASI 2022-2024, implique para la prestación puntual de dichos servicios.

En todos los casos, los servicios se aceptarán siempre y cuando la totalidad de los componentes habilitadores, y sus funcionalidades requeridas, hayan sido correctamente entregadas y aceptadas por el Administrador del Contrato y las áreas del Instituto que deban involucrarse, dependiendo de la naturaleza del servicio.

El proveedor del servicio de SASI 2022-2024, deberá considerar que el Instituto proveerá los servicios de energía eléctrica y hosting en los centros de datos y localidades donde residirán los componentes habilitadores requeridos para soportar cada uno de los servicios de SASI 2022-2024. Los insumos necesarios para la instalación, energización y todos los componentes de *hardware* y *software* necesarios para la incorporación de las soluciones propuestas por el licitante ganador a la red del Instituto, será a cargo del licitante adjudicado.

Para la instalación, configuración y habilitación de cada una de las soluciones de los servicios, el proveedor de SASI 2022-2024, deberá considerar el apego a los procesos y procedimientos de control de cambios del Instituto para la integración de la infraestructura los Centros de Datos del Instituto. El detalle de estos procesos y procedimientos se proporcionarán en las Mesas de Trabajo entre el licitante ganador de SASI 2022-2024, y el Instituto.

Es importante señalar que, el licitante adjudicado deberá contar con un proceso para la gestión de solicitudes que impliquen cualquier tipo de modificación o cambio en los componentes habilitadores requeridos en la descripción particular de cada uno de los servicios; para tal efecto, el licitante ganador deberá entender el

control de cambios como la función de agregar, remover o modificar debidamente los componentes habilitadores y/o las configuraciones que lo necesiten, con la finalidad de ejecutar algún cambio orientado a satisfacer las necesidades del Instituto, sin afectar la continuidad de la operación, del negocio o de la seguridad de la información.

### 6.6. Implementación de los servicios

Las obligaciones contractuales mínimas del proveedor adjudicado, sin menoscabo de realizar aquellas que no estén incluidas en este apartado y que sean necesarias para cumplir con los requerimientos de servicio de SASI 2022-2024, son las siguientes:

- **Implementación de Servicios**: corresponde a la provisión, entrega, montaje e instalación física y lógica de todos los componentes de hardware, software, así como y puesta en marcha de todas las funcionalidades requeridas para cada uno de los servicios. Esto incluye conexiones a la red eléctrica e integración a la Red, así como asegurar la interoperabilidad con el resto de los componentes del Centro o los Centro de Datos del Instituto y ejecución de pruebas a nivel red y aplicativo, los componentes, equipos, accesorios, herramientas y todo lo necesario para el cumplimiento del presente apartado, debe quedar incluido en la propuesta del licitante ganador.

- **Migración de servicios Seguridad**: Corresponde a la responsabilidad de entregar un plan de migración, así como las correspondientes actividades en las que involucra migración de flujos de seguridad que se deben brindar en los componentes habilitadores que el proveedor de SASI 2022-2024, proveerá al Instituto. Estas actividades involucra a las tecnologías de conmutación, enrutamiento, centro de datos, seguridad, sin menoscabo de migrar aquellos flujos que no estén incluidas en este apartado y que sean necesarias para la entrega correcta del plan de migración requeridas en este proyecto, siendo los proveedores salientes quienes entreguen los flujos de comunicación y seguridad necesarios al proveedor de SASI 2022-2024, en forma documental al gobierno de contrato y áreas de tecnología involucradas del Instituto antes de comenzar las labores de implantación para su validación.

- **Operación estable del proyecto**: Pruebas integrales de todas las funcionalidades de los Componentes Habilitadores y la conectividad e interoperabilidad con el resto de los Componentes del Centro de Datos. El proveedor adjudicado llevará a cabo la integración y pruebas de la infraestructura de Comunicaciones, Seguridad, *software* y de las herramientas asociadas que aseguren que toda la infraestructura y componentes que conforman, se encuentren operando correctamente como un solo sistema integral (pruebas de conectividad, reglas de flujos de comunicaciones, políticas de seguridad, funcionalidades, seguridad, monitoreo y gestión).

### 6.7. Mesas de Trabajo

El proveedor adjudicado será responsable de integrar al servicio de SASI 2022-2024, una mesa de trabajo para la atención de los diferentes requerimientos que puedan surgir durante la vigencia del contrato.

Este servicio deberá estar disponible a lo largo de la vigencia del presente contrato. De este modo, el licitante adjudicado será el responsable de asignar personal con experiencia y expertos para conformar las mesa de trabajo. En caso de que el personal asignado sea retirado del servicio de SASI 2022-2024, será responsabilidad del licitante adjudicado notificar al Instituto con anticipación el motivo y fecha de su remoción

de manera oficial. Así también será responsable de notificar de qué manera se llevará a cabo la sustitución del recurso en un esquema que garantice siempre la continuidad y calidad de los servicios requeridos.

El proveedor adjudicado será responsable de instrumentar las mesas de trabajo tanto para las funcionalidades que utilice la infraestructura, así como también aquellas que impliquen una reingeniería de la misma, en las que se desarrollarán reportes de evaluación de postura de redes y seguridad del servicio, se documentarán conclusiones y recomendaciones de modificación de la infraestructura de la red y seguridad como mejora u optimización de la disponibilidad, capacidad y desempeño de los recursos y seguridad de las aplicaciones que vivan en los centros de datos del Instituto.

El Instituto podrá en cualquier momento de la vigencia del contrato de SASI 2022-2024, solicitar al proveedor adjudicado del servicio de diseño para cambios relevantes que se planeen efectuar en la infraestructura de red y seguridad que conforman el presente proyecto.

A continuación, se enlistan las responsabilidades mínimas que tendrá que llevar a cabo el licitante adjudicado, sin menoscabo de realizar aquellas que no estén incluidas en este apartado y que sean necesarias para cumplir con los requerimientos solicitados.

- Generar reportes de estado de salud y proponer mejoras y/o soluciones arquitectónicas de la infraestructura de red y seguridad.
- Análisis de impacto de nuevos requerimientos que requieran el uso de la Infraestructura de red y seguridad existente en el contrato de SASI 2022-2024.
- Desarrollo de recomendaciones de optimización de anchos de banda, mejores rutas, optimización de la infraestructura.
- Diseño de mejoras sobre la infraestructura y recomendaciones que brinden el más alto desempeño y nivel de servicio.
- Entrega de reportes proactivos de recomendaciones de actualizaciones de software de los componentes habilitadores que conforman el contrato SASI 2022-2024.
- Entrega de reporte de análisis detallado del comportamiento de la red de comunicaciones y elementos de seguridad que conforman el contrato SASI 2022-2024.
- Todas las propuestas de configuración avanzada o configuración de nuevas funcionalidades propuestas por el licitante ganador de SASI 2022-2024 deben de estar validadas por personal certificado y con experiencia del proveedor del servicio de SASI 2022-2024.
- Consultoría y recomendaciones de arquitectura de Centro de Datos en base a sus mejores prácticas, dimensionamiento, uso adecuado de recursos.
- Revisión de los requerimientos de diseño, prioridades y objetivos de acuerdo a lo especificado por el administrador del contrato.
- Revisión de la arquitectura y topología de la infraestructura de la red.
- Revisión de la configuración de protocolos.
- Revisión de la configuración de características de los servicios.
- Revisión de las mejores practicas en materia de seguridad informática.
- Recomendación y diseños que permitan incrementar de manera notable las funcionalidades y que conforman la infraestructura tecnológica del Instituto.

### 6.8. Perfil del Proveedor

El proveedor deberá contar con la capacidad, flexibilidad, solvencia económica y competencia técnica certificada que permita implementar y operar las soluciones de seguridad y sus mecanismos con todo lo necesario para su correcto funcionamiento, en los sitios en donde "EL INSTITUTO" lo requiera conforme a las características y especificaciones mencionadas en el presente Anexo Técnico.

El personal del proveedor del servicio, que atenderá las operaciones de los servicios de seguridad, deberá contar con experiencia probada en las áreas de tecnología y de seguridad de la información previamente mencionadas, para lo cual, deberá integrarse el currículo vitae de todo el personal que participe en el servicio, indicando al menos:

- Experiencia profesional: bajo este rubro, se considerarán todos los puestos que cada integrante haya desempeñado, con fecha, nombre de los empleadores, nombre de los puestos que ha ejercido y el tipo de funciones bajo su responsabilidad, y deberá contar con experiencia comprobable al menos 3 años.
- Experiencia en proyectos de su especialidad en Seguridad de la Información: bajo este rubro se citarán y describirán todos los proyectos en que se ha participado, y deberá contar con experiencia comprobable de al menos 3 años.
- Estudios: bajo este rubro se anotarán todos los estudios en materia de seguridad de la información, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica. Las certificaciones son de tecnología y/o de seguridad de tipo "vendor-neutral".
- Incluir la estructura del grupo de trabajo, indicando por cada perfil las responsabilidades y competencias.

El currículo vitae de todo el personal que participe en el servicio, se acreditara siempre y cuando contenga todas y cada una de las características requeridas, por lo que el incumplimiento de la presentación de este, afectaría la solvencia de la propuesta.

Se deberá acreditar al menos la licenciatura o ingeniería en informática, telecomunicaciones, computación o carrera a fin, en los términos que establece la Ley Reglamentaria del Art. 5 Constitucional, la acreditación será con el título y cédula profesional y para el caso de estudios en el extranjero, estos deberán estar avalados por las instancias oficiales correspondientes, así como estar debidamente apostillados.

A continuación, se listan las credenciales y capacidades que deberán cubrir los recursos asignados al proyecto:

**Partida 1**

## Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

| Perfil | Certificaciones a demostrar | Experiencia a desmostrar | Función | Número de recursos |
|---|---|---|---|---|
| Administrador del Centro de Operaciones de Seguridad (SOC) | Se deberá presentar alguna las siguientes certificaciones vigentes:<br><br>CISM (Certified Information Security Manager)<br>CISSP (Certified Information Systems Security Professional)<br>CRISC (Certified in Risk and Information Systems Control) | 3 años de experiencia en participación de proyectos de seguridad de la información. | Responsable de la administración, monitoreo, operación de los servicios proporcionados por el SOC, así como del soporte, atención a fallas e incidentes de seguridad | Al menos 1 |
| Administración y Operación de soluciones y herramientas tecnológicas | Consultor especializado en cada una de las soluciones de seguridad integradas. Se aceptan como documentos comprobables el certificado vigente que haya tomado directamente del fabricante o de un centro de entrenamiento autorizado por el fabricante. | 3 años de experiencia en participación de proyectos de seguridad de la información. | Operar administrar y monitorear las soluciones de seguridad propuestas. | Al menos 3 |
| Líder de proyecto | Se deberá presentar alguna las siguientes certificaciones vigentes:<br><br>PMP (Project Manager Professional) Certificado por PMI<br>ITIL v4 (Expert o Master)<br>EC-Council Project Management In IT Security (PMITS) | 3 años de experiencia en participación de proyectos de seguridad de la información. | Es la persona encargada de administrar y coordinar el proyecto | Al menos 1 |
| Operador de la mesa de servicio SOC | Se deberá presentar la siguiente certificación vigente:<br><br>ITIL v4 Foundation Certification | 3 años de experiencia en participación de proyectos de seguridad de la información. | Personal encargado de las operaciones de soporte de primer nivel, el monitoreo de los servicios, así como del registro y seguimiento de solicitudes de ventanas de mantenimiento, reportes de fallas y requerimientos | Al menos 4 |

| Perfil | Certificaciones a demostrar | Experiencia a desmostrar | Función | Número de recursos |
|---|---|---|---|---|
| Arquitecto Especializado en Redes y Seguridad | Se deberá presentar alguna las siguientes certificaciones vigentes:<br><br>CCNP (Cisco Certified Network Professional)<br>CCIE Enterprise Infrastructure (Cisco Certified Internetwork Expert)<br>CCIE Security (Cisco Certified Internetwork Expert) | 3 años de experiencia en participación de proyectos de redes y seguridad de la información. | Responsable de la administración, monitoreo, operación de los servicios proporcionados por el SOC, en lo que a servicios de interconexión de red se refiere, así como del soporte, atención a fallas e incidentes que se presenten en la interoperabilidad con otros proveedores y/o fabricantes | Al menos 1 |

## Partida 2

| Perfil | Certificaciones a demostrar | Experiencia a desmostrar | Función | Número de recursos |
|---|---|---|---|---|
| Líder de proyecto | Se deberá presentar alguna las siguientes certificaciones vigentes:<br><br>PMP (Project Manager Professional) Certificado por PMI<br>ITIL v4 (Expert o Master)<br>EC-Council Project Management In IT Security (PMITS) | 3 años de experiencia en participación de proyectos de seguridad de la información. | Es la persona encargada de administrar y coordinar el proyecto | Al menos 1 |
| Analista de Seguridad | Se deberá presentar la siguiente certificación vigente:<br><br>CEH (Certified Ethical Hacker) | 3 años de experiencia en participación de proyectos de seguridad de la información. | Responsable de ejecutar las revisiones de seguridad sobre las aplicaciones y la infraestructura, así como prever, detectar, analizar, contener, erradicar, documentar incidente de seguridad | Al menos 2 |

| Perfil | Certificaciones a demostrar | Experiencia a desmostrar | Función | Número de recursos |
|---|---|---|---|---|
| Consultor de Penetración | Se deberá presentar alguna las siguientes certificaciones vigentes:<br><br>GPEN (GIAC Certified Penetration Tester)<br>CEH (Certified Ethical Hacker) | 3 años de experiencia en participación de proyectos de seguridad de la información. | Realizar simulacros de ataque a la red de la infraestructura o las aplicaciones para determinar lo que los atacantes pueden acceder y qué problemas pueden causar<br><br>Evaluar la seguridad de la infraestructura de red y aplicaciones utilizando herramientas y técnicas que un atacante podría utilizar | Al menos 1 |
| Consultor Forense de Cómputo | Se deberá presentar alguna las siguientes certificaciones vigentes:<br><br>EnCE (EnCase Certified Examiner)<br>CHFI (Certified Hacker Forensics Investigator) | 3 años de experiencia en participación de proyectos de seguridad de la información. | Analizar, en el supuesto de un ataque y penetración exitoso a la infraestructura, la metodología de ataque para determinar cómo se logró, cuál fue el alcance del daño, logrando así determinar las medidas preventivas a implementar.<br>Debe tener la capacidad de ejecutar investigaciones forenses en caso de ser necesario | Al menos 1 |

## 7. Condiciones técnicas de aceptación de entregables

Durante la habilitación, transición y operación de los servicios de seguridad, el Instituto requiere recibir distintos tipos de documentos, reportes, artefactos, dictámenes o esquemas que favorezcan el desempeño y la continuidad del servicio, y que den certidumbre a las actividades diarias que el proveedor efectuará bajo la supervisión de los funcionarios designados por este último para tales efectos.

### 7.1. Entregables Generales

Durante la habilitación, transición y operación de los servicios de seguridad, el Instituto requiere recibir distintos tipos de documentos, reportes, artefactos, dictámenes o esquemas que favorezcan el desempeño y la continuidad del servicio, y que den certidumbre a las actividades diarias que el proveedor efectuará bajo la supervisión de los funcionarios designados por este último para tales efectos.

### Partida 1

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Habilitación, Operación y Transición | Plan de Trabajo Detallado de los servicios del proyecto | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Documento Compromiso de suscripción del acuerdo de niveles operacional (*Operational Level Agreement,* OLA) | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Matriz de Escalación | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| Servicios de Seguridad – Continuidad Operativa | Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto | Única Vez | 5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | donde lo indique el Instituto | | |
| | Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas | Única Vez | 10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo |
| | Memorias Técnicas Actualizadas de las Servicios de Seguridad | Única Vez | 20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados |
| Servicios de Seguridad – Verificación/Calidad | Documento con el diseño de Alto Nivel de los servicios de Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integran activos de infraestructura para su habilitación | Única Vez | 5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integran | Única Vez | 10 días hábiles posteriores al término de la habilitación de todos los componentes en los |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | activos de infraestructura para su habilitación | | Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo |
| | Memorias Técnicas Actualizadas de las Servicios de Seguridad, que requieran integran activos de infraestructura para su habilitación | Única Vez | 20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados |
| Servicios de Borrado Seguro de Información | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicio de Gestión de Dominios | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicio de Certificados Digitales SSL | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Sistema de Gestión de Seguridad de la Información (SGSI) | Metodología para la continuidad de los servicios | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Gestión del Cambio en Seguridad de la Información | Metodología para la implementación de los servicios | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Procesos de operación implementados: | Única Vez | 15 días naturales posteriores a la emisión del fallo |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | • Requerimientos<br>• Cambios<br>• Configuraciones<br>• Incidentes<br>• Problemas<br>• Monitoreo | | |
| | Matriz de Escalación Técnica y Organizacional | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Procedimiento de operación de la Mesa de Servicios:<br>• Requerimientos<br>• Cambios<br>• Configuraciones<br>• Incidentes<br>• Problemas<br>• Monitoreo | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Expedientes Curriculares del personal del SOC | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| Tablero de Estadísticas de Servicios de Seguridad (Portal Único) | Creación de cuentas de acceso en portal único de las soluciones de seguridad | Única Vez | 10 días hábiles posteriores al término de la habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo |

**Partida 2.**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Habilitación, Operación y Transición | Plan de Trabajo Detallado de los servicios del proyecto | Única Vez | 15 días naturales posteriores a la emisión del fallo |

| | | | |
|---|---|---|---|
| | Documento Compromiso de suscripción del acuerdo de niveles operacional (*Operational Level Agreement,* OLA) | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Matriz de Escalación | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| Servicios de Análisis de Vulnerabilidades Dinámico | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Pruebas de Penetración | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Análisis Forense | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Análisis de Vulnerabilidades Estático | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |

### 7.2. Entregables bajo demanda

El proveedor, de manera enunciativa más no limitativa, deberá generar entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

**Partida 1.**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Borrado Seguro de Información | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado. | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicio de Gestión de Dominios | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos. | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicio de Certificados Digitales SSL | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los certificados que se hayan renovado o adquiridos (incluyendo archivo | Evento | 1 día hábil posteriores a la solicitud generada por parte del Instituto |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | electrónico compreso con la llave publica relacionado con los requerimientos) | | |
| Servicios de Sistema de Gestión de Seguridad de la Información | Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo | Evento | 10 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicios de Gestión del Cambio en Seguridad de la Información | Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo | Evento | 10 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad | Evento | 5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto |
| | Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad | Evento | 5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme cada solicitud generada por el Instituto |
| | Actualización de la matriz de escalación | Evento | 5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad y Red |
| | Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad y red | Evento | 5 días hábiles posteriores a la ejecución de la ventana mantenimiento |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad y red | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Reporte Técnico de las configuraciones de las soluciones de seguridad y red | Evento | 5 días hábiles posterior a la solicitud generada por parte del Instituto |
| | Reporte Técnico de los incidentes presentados en las soluciones de seguridad y red | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Reporte Técnico de los requerimientos registrados en la mesa de servicios | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y red, así como su diagrama de interrelación conforme fueron registrados en la CMDB | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Diagramas de Arquitectura de las soluciones de seguridad y red | Evento | 2 días hábiles posteriores a la solicitud generada por parte del Instituto |

**Partida 2**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Análisis de Vulnerabilidades Dinámico | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de | Evento | 7 días hábiles posteriores a la solicitud generada por parte del Instituto |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis | | |
| Servicios de Prueba de Penetración | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas | Evento | 10 días hábiles posteriores a la solicitud generada por parte del Instituto |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | para el proceso de análisis | | |
| Servicios de Análisis Forense | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de infraestructura verificados | Evento | 15 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicios de Análisis de Vulnerabilidades Estático | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada pieza de software (codigo) analizados indicando al menos: aplicativo relacionado, fecha de análisis, código fuente analizado, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis | Evento | 10 días hábiles posteriores a la solicitud generada por parte del Instituto |

**7.3. Entregables Periódicos**

El proveedor, de manera enunciativa más no limitativa, deberá generar entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

## Partida 1

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Seguridad – Continuidad Operativa | Reportes Técnicos de los activos de infraestructura que contemplen:<br>• Disponibilidad<br>• Controles de Cambios<br>• Requerimientos<br>• Incidentes/Fallas<br>• Actividad Sospechosa<br>• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| Servicios de Seguridad – Verificación/Calidad | Reportes Técnicos de los activos de infraestructura que contemplen:<br>• Disponibilidad<br>• Controles de Cambios<br>• Requerimientos<br>• Incidentes/Fallas<br>• Actividad Sospechosa<br>• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte Técnico de los eventos de actividad sospechosa presentados | Mensual | 5 días hábiles posteriores al |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | en los servicios de seguridad implementados | | cumplimiento del mes vencido |
| | Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte de las evaluaciones operativas a los servicios de seguridad implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |
| | Reporte que integre el calendario de actualizaciones de versionamiento en *software* de cada servicio implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |

**Partida 2**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Análisis de Vulnerabilidades Dinámico<br><br>Servicios de Análisis de Vulnerabilidades Estático<br><br>Servicios de Pruebas de Penetración<br><br>Servicios de Análisis Forense | Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte de las evaluaciones operativas a los servicios de seguridad implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |
| | Reporte que integre el calendario de actualizaciones de | Trimestral | 5 días hábiles posteriores al |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | versionamiento en *software* de cada servicio implementados | | cumplimiento de cada trimestre calendario |

Los entregables requeridos durante la vigencia del contrato, deberán ser entregados en formato electrónico (MS Word, MS Excel, PDF) conforme los periodos estipulados por el Instituto.

De igual manera, el proveedor deberá establecer un repositorio digital, que, de manera alterna, servirá para alojar los entregables antes señalados, mismos que estarán disponibles para su consulta durante la vigencia del contrato, teniendo en cuenta que el Instituto definirá en las mesas de trabajo los permisos de acceso correspondientes para el administrador del contrato, cuerpo de gobierno que se conforme para este propósito u otros funcionaros que sean designados por el primero mencionado.

**8. Niveles de servicio que deberán cumplirse (SLA)**

El objetivo de los Niveles de Servicio consiste en proporcionar al Instituto un mecanismo que permita:

- Medir de forma efectiva el desempeño de los servicios proporcionados por el proveedor.
- Procurar que los servicios de sean proporcionados con la calidad prevista.

Los Niveles de Servicio son métricas definidas por el "IMSS" que serán cumplidas por el proveedor de SASI 2022-2024, con objeto de cumplir con la calidad requerida en la prestación del servicio.

Con relación a lo establecido en los artículos 45, fracción XIX, 53 y 53 BIS de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 86, segundo párrafo, 95, 96 y 97 de su Reglamento; se aplicarán las Penas Convencionales y Deducciones correspondientes, por atraso en el cumplimiento de las fechas pactadas de entrega o de la prestación del servicio y, con motivo del incumplimiento parcial o deficiente en que pudiera incurrir el "Proveedor" de SASI 2022-2024, respecto de los servicios prestados.

Los niveles de servicios se aplicarán conforme a lo estipulado en el documento de "Términos y Condiciones".

**8.1. Penas Convencionales**

Durante la vigencia del contrato, se aplicarán penas convencionales a todos aquellos servicios que no sean entregados conforme lo establecido en los niveles de servicios definidos por el instituto.

Las penas convencionales se aplicarán conforme a lo estipulado en el documento de "Términos y Condiciones".

**9. Deducciones**

Durante la vigencia del contrato, al presentarte una falla, incidente, atención de requerimientos, ventana de mantenimiento, entre otras, cuya causa raíz haya sido derivada por un tercero, la deductiva correspondiente al servicio asociado no será aplicada al proveedor de SASI 2022-2024, siempre y cuando demuestre con

evidencias fehacientes que el servicio correspondiente se presentó bajo las especificaciones del anexo técnico y sus apéndices.

Con base en lo anterior, y cuando las fallas, incidentes, atención de requerimientos, ventanas de mantenimiento, entre otras, sean atribuibles a la entrega de los servicios de seguridad por parte del Proveedor se aplicara una deductiva conforme los niveles de servicios establecidos,

Las deducciones se aplicarán conforme a lo estipulado en el documento de "Términos y Condiciones".

**10. Convenio de Confidencialidad y Resguardo de la Información**

El "Licitante" deberá suscribir el Convenio de Confidencialidad y Resguardo de Información correspondiente. En complemento, el "Licitante" deberá considerar al menos los siguientes mecanismos de control de acceso a la información del IMSS:

a. Se deberán establecer controles de acceso y privilegios restringidos al personal del "Licitante", a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del IMSS.

b. El "Licitante" deberá implantar y aceptar en todo momento el uso de controles que permitan establecer "Pistas de Auditoria" para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.

c. Los empleados del "Licitante" con acceso a la información sensible del IMSS, deberán firmar acuerdos de confidencialidad con este.

d. El almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por el instituto de los servicios de SASI 2022- 2024 observando los requisitos de seguridad y resguardo de la información.

e. El "Licitante" deberá permitir el acceso a información relacionada con el servicio prestado al IMSS para la realización de auditorías.

f. El "Licitante" no deberá hacer uso indebido de la documentación, información, ni activos de TIC a los que tengan acceso o que se generen con motivo de la prestación del servicio.

**11. Normas**

No aplica

**12. Normatividad Aplicable**

El Proveedor de servicios deberá sujetarse a las políticas internas vigentes del Instituto y a cualquier modificación o inclusión de nuevas políticas que se realicen durante la vigencia del contrato. Las políticas aplicables se le darán a conocer durante las mesas de trabajo, sin embargo, se deberán considerar las que se enlistan a continuación, de manera enunciativa más no limitativa:

- Marco normativo de aplicación general y obligatoria en la Administración Pública Federal.
- Artículo 8, segundo y tercer párrafo, fracción I de la Ley Orgánica de la Administración Pública Federal.
- Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la Información y comunicación, y la seguridad de la información en la Administración Pública Federal.
- Políticas de Seguridad con base en el Sistema de Gestión de Seguridad de la Información (SGSI) del Instituto.
- Certificados ISO/IEC27001:2013 e ISO/IEC20000-1:2018 vigentes a nombre del licitante participante.

**13. Cumplimiento de Políticas**

El Proveedor de servicios deberá respetar las políticas de seguridad vigentes en el Instituto y bajo ninguna circunstancia permitirá que se infrinjan los lineamientos vigentes. Si alguno de los lineamientos de seguridad implantados en el Instituto llegase a cambiar durante la vigencia del contrato establecido con dicho proveedor, éste deberá asegurarse de modificar su infraestructura y procesos de tal forma que cumpla con los nuevos requerimientos.

Todos los equipos de cómputo personal propiedad del proveedor de servicios, que estén involucrados en la prestación de los servicios, deberán estar protegidos con sistemas de detección de intrusos, control de infecciones virales, detección y eliminación de programas tipo "back door" o "Troyanos". Esta regla aplica tanto para los equipos de cómputo móviles (laptops, handheld, smartphones, tablet PC, etc.) como para los equipos de escritorio (desktop, deskside, etc.) usados por los recursos designados para las diversas tareas de administración y gestión.

Si dichos equipos requieren de la instalación de sistemas operativos, aplicaciones, sistemas antivirus, sistemas de seguridad y demás herramientas que el proveedor considere necesario para la correcta operación de su personal, así como de la adquisición, instalación, mantenimiento y licenciamiento de estos, el costo será absorbido por el proveedor.

**14. Finalización del Contrato**

En el caso de terminación anticipada del contrato o a la finalización de la vigencia del mismo, el "Licitante" será responsable de iniciar el proceso de respaldo de la información, el proceso de baja, de realizar los movimientos de resguardo, traslado y empaquetado de todo el equipo ubicado en las instalaciones del IMSS que forma parte de los servicios y que no constituya parte de las modificaciones, adecuaciones y/o activos que hayan sido realizados como permanentes, o aquellos que de común acuerdo con el IMSS hayan sido sustituidos como parte del servicio.

Una vez terminada la vigencia del servicio, la infraestructura, los componentes habilitadores y los demás elementos utilizados por el proveedor para la prestación de los servicios se transferirán al IMSS para la continuidad operativa. Este acto se llevará a cabo mediante un acta de entrega recepción, en la que dichos componentes se transmitirán al IMSS, a título gratuito, libres de toda limitación de dominio, gravamen y responsabilidad de cualquier naturaleza, conforme a la normativa aplicable al Instituto.

El "Licitante" deberá entregar al IMSS, a más tardar 2 meses antes de la finalización del contrato, un plan de trabajo detallado para lograr una transición efectiva de los servicios de seguridad, en el que se incluyan todos aquellos elementos para efectuarlo. Dicho plan deberá permitir una completa y correcta transición de los servicios, incluyendo la conformación y actualización de la documentación necesaria del proyecto, asi como las mesas de trabajo necesarias para dicha transición con el o los proveedores que den continuidad operativa al proyecto.

La documentación deberá incluir información que se generó durante la vigencia del contrato, documentación de los procesos internos de aprovisionamiento, configuración y tareas de operación, soporte y mantenimiento debidamente actualizadas, tomando en consideración los eventos de administración de cambios y configuración, incidentes y problemas, además de un inventario actualizado a la fecha de entrega de todos los componentes habilitadores e infraestructura auxiliar que el IMSS solicite se mantengan para la transición de un nuevo contrato de servicios, para que pueda continuarse prestando el mantenimiento preventivo y correctivo a todos los componentes de la solución y diseñar el mecanismo para la renovación tecnológica del resto, procurando afectar de forma mínima la operación.

La fecha límite para la entrega de la documentación final actualizada que se mencionó anteriormente será de 2 meses antes de la finalización del contrato SASI 2022-2024. Asimismo, el "Licitante" deberá implementar un esquema de respaldo de la información en cada uno de los componentes que integran los servicios incluyendo los relacionados con los Centros de Datos del IMSS, el respaldo de la información deberá ser almacenada en cada punto táctico para ser entregada al cuerpo de gobierno del contrato para su resguardo. Una vez contando con la autorización del cuerpo de gobierno de SASI 2022-2024.

Asimismo, al término del contrato, garantizará los niveles de servicio durante el período de transferencia de servicios al nuevo proveedor.

Dicho período de transición estará sujeto al plan de trabajo que el "Licitante" haya presentado previamente, y que el IMSS hubiera aprobado. No obstante, durante dicho periodo, el "Licitante" deberá proporcionar la orientación tecnológica adecuada al personal del IMSS para garantizar la continuidad de los servicios requeridos, poniendo a disposición del IMSS o de un tercero la transferencia.

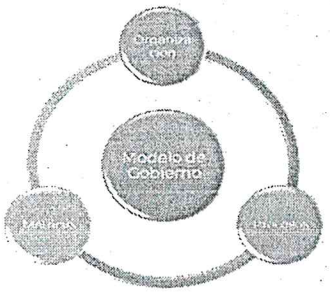
**15. Modelo de Gobierno**

El Modelo de Gobierno establece la forma como se trabajará en relación con este proyecto, los lineamientos operacionales para el proveedor y la manera como se medirá el grado de desempeño. El Modelo de Gobierno surge de la necesidad de diseñar una estructura operativa orientada a procesos para administrar los "Servicios Administrados de Seguridad Informática SASI 2022-2024", el cual facilitará la relación entre todos los involucrados para su adecuada implantación y operación.

El Modelo de Gobierno comprende los principales aspectos a considerar para asegurar y controlar la operación del proyecto.

Dicho modelo establece la organización y los roles que participarán por parte del Instituto dentro del proyecto.

El Modelo de Gobierno establece esquemas operativos y procesos, con la finalidad de que cada una de las etapas del servicio, el administrador del contrato y los lideres del proyecto, con apoyo por parte del proveedor del servicio (SOC), garanticen los niveles de servicios establecidos para la operación.




La estructura organizacional que ejecutar para el proyecto de "Servicios Administrados de Seguridad Informática (SASI 2022-2024)", busca que los responsables trabajen de manera efectiva, definiendo roles y responsabilidades en cada nivel, para lo cual se muestra en la siguiente tabla de manera enunciativa mas no limitativa a los responsables y sus roles correspondientes.

| NIVELES ORGANIZACIONALES | RESPONSABLES | DESCRIPCIÓN |
|---|---|---|
| Supervisión y Administración de los Servicios | • Administración de Contrato | Determinar los incumplimientos respecto a las penas convencionales y/o deductivas descritas en Anexo Técnico, Términos y Condiciones en el apartado "Acuerdos de Niveles de Servicio de SASIC"<br><br>Elaborar el dictamen de servicios, el cual deberá contener los servicios prestados a mes vencido, así como la identificación de los incumplimientos de los mismos. |
| Líder de Proyecto Proveedor (SOC) | • Líder del proyecto del proveedor | Entregar al administrador del contrato la documentación relativa a los servicios bajo su responsabilidad ("Reporte de Servicios Consolidado" y "Reportes de Niveles de Servicios" correspondientes). |
| Líder de Proyecto Operación | • Líderes de los Servicios del proyecto SASIC | Mantener la operación de los servicios de acuerdo a los niveles de servicio establecidos en descritas en Anexo Técnico, Términos y Condiciones en el apartado "Acuerdos de Niveles de Servicio de SASIC". |

# Apéndice "A"

# Servicios Administrados de Seguridad Informática (SASI) 2022-2024

## 1. Objetivo del Documento

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

## 2. Servicio de Firewall

Especificaciones Técnicas:

- Cumplir con el desempeño y capacidades considerando al menos las siguientes especificaciones:

| | Tipo 1 | Tipo 2 | Tipo 3 | Tipo 4 |
|---|---|---|---|---|
| Desempeño | 5 Gbps | 10 Gbps | 20 Gbps | 240 Gbps |
| Conexiones simultaneas por seg. | 1,000,000 | 2,000,000 | 4,000,000 | 32,000,000 |
| Conexiones nuevas por seg. | 50,000 | 125,000 | 200,000 | 1,000,000 |
| Paquetes por seg. | 1,000,000 | 3,000,000 | 5,000,000 | 30,000,000 |
| Interfaces 10GbE | 8 | 8 | 12 | 12 |

Se requieren mínimo 2 y máximo 4 equipos tipo 4 para el centro de datos principal, ubicado en Morelia Michoacán (configuración en HA)

- El licitante deberá considerar en su propuesta económica que las características de conexiones simultaneas por segundo se refiere a conexiones concurrentes por segundo.
- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
- Certificado por organismos de la industria como Common Criteria o ICSA Labs.
- Incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permitir implementar reglas aplicadas a intervalos de tiempo específicos.
- Integrar listas de control de acceso basadas en dirección origen, dirección destino, protocolos, interfaces de red, puertos, URL destino, identidad, rangos de tiempo o periodo.

- Capacidad de agrupar objetos tales como direcciones IP, protocolos y puertos para la simplificación de configuración de políticas de seguridad.
- Capacidad de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con tiempo de espera agotado (timeout).
- Capacidad de implementar mecanismos de calidad de servicio tales como la asignación de ancho de banda a cada tipo de flujo, encolamiento prioritario y moldeado de tráfico (traffic shaping).
- Capacidad de inspeccionar tráfico FTP, HTTP, HTTPS, DNS, ICMP, RADIUS, SMTP y SNMP, H.323, SIP, RSTP, SNMP, entre otros.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Capacidad de segmentar lógicamente el o los activos de infraestructura en dispositivos virtuales (firewalls virtuales); en el que cada instancia virtual es un dispositivo independiente con sus propias políticas de seguridad, interfaces y usuarios administrativos.
- Capacidad de crear hasta 100 instancias de dispositivos virtuales (firewalls virtuales) que deberán ser soportadas en cada uno de los diferentes tipos de firewalls.
- Deberá soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
- Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
- Soportar y operar bajo protocolos de ruteo BGP y OSPF.
- Soportar y operar mediante rutas estáticas.
- Realizar inspección en capa 3 y 4.
- Soporte y operación con al menos 1,000 VLANs
- Integrar esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Contar y operar al menos con una interface Gigabit Ethernet dedicada para administración.
- Generación de bitácoras de eventos (logs) con múltiples niveles de criticidad.
- Incluir una consola centralizada de gestión con las siguientes características:
    - Configuración, de manera centralizada, de políticas en todos los firewalls de la infraestructura.
    - Identificación de qué reglas corresponden a fuentes, destinos y tipos de tráfico.
    - Ejecución de operaciones para grupos o bloques de dispositivos de frontera de seguridad.
    - Capacidad de ofrecer diferentes vistas durante el monitoreo de dispositivos, topologías o políticas.
    - Agrupación de parámetros de configuración para su posterior implementación.
- Durante una actualización de configuración, deberá ser capaz de regresar a la configuración anterior, si es necesario o requerido.
- Auditoria de todas las actividades realizadas por los usuarios con privilegios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.

**3. Servicio de Prevención de Intrusos (IPS)**

Especificaciones Técnicas:

- Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

| | Tipo 1 | Tipo 2 | Tipo 3 |
|---|---|---|---|
| Desempeño | 15 Gbps | 20 Gbps | 24 Gbps |
| Conexiones simultaneas / concurrentes por seg. | 15,000,000 | 25,000,000 | 30,000,000 |
| Conexiones nuevas por seg. | 120,000 | 160,000 | 200,000 |
| Interfaces 10GbE | 4 | 8 | 8 |

Se requieren mínimo 2 y máximo 4 equipos tipo 3 para el centro de datos Principal ubicado en Morelia Michoacán (configuración en HA)

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Latencia máxima de 0.5 milisegundos.
- Las interfaces de Inspección deberán operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
- Capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado.
- Capacidad de detección en línea sin bloquear tráfico (Modo transparente o supervisión). El sistema sólo alertará que eventos serían bloqueados.
- Capacidad de configuración del modo transparente o supervisión para todo el tráfico o sólo para los paquetes especificados por dirección IP, protocolo, VLAN ID, entre otros.
- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.
- Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
- Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.
- La solución de IPS deberá contemplar que el flujo de información esté asegurado ante una falla en el IPS, pudiendo conmutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.
- Soporte de funcionalidades de alta disponibilidad y configuraciones del tipo activo/activo y activo/failover. Esto deberá ser soportado sin degradar el desempeño del IPS y manteniendo las tasas de transmisión requerida.
- Soporte de actualizaciones automáticas de seguridad del archivo de firmas de cuando menos una vez por mes.
- Soporte de análisis de tráfico de voz sobre IP.
- Soporte de monitoreo de VLANs, incluyendo tramas 802.1q
- Soporte de monitoreo de IPv6.
- Soporte de monitoreo con inspección profunda de paquete y monitoreo de paquete en escenarios de alta disponibilidad y con handshake TCP incompleto.

- Reconocimiento de Tuneleo de Protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
- Detección de escaneo de puertos.
- Detección de re-ensamblaje de paquetes fragmentados.
- Captura de tráfico para el análisis de evidencia en formato soportado por TCPDUMP y de manera opcional en formato. ENC (estándar para el software de análisis de protocolos), dicho archivo podrá ser usado para hacer reconstrucción o análisis forense del ataque.
- Integración de Listas Blanca (IP whitelist) mediante una lista de direcciones IP "confiables" que el sistema no bloqueará.
- Integración de firmas definidas por el Instituto mediante el uso de expresiones regulares.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos hosts de la red y crear una alarma cuando cierto umbral sea rebasado.
- Capacidad de integración con el directorio de usuarios (Active Directory y/o LDAP).
- Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
- Administración de seguridad centralizada que incluya las políticas, actualización, respuestas (bloquear, notificar, ignorar, etc.) y opciones de auditoría.
- Consola centralizada que administre los IPS y la integración de usuarios que realice las configuraciones necesarias para remediación de incidentes de seguridad.
- Consola remota con interfaz gráfica o Web cifrada (HTTPS) para el uso en modo de consulta, con diferentes perfiles de usuarios.
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
- Deberá soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
- Capacidad de segmentar lógicamente el o los activos de infraestructura en dispositivos virtuales (IPS virtuales); en el que cada instancia virtual es un dispositivo independiente con sus propias políticas de seguridad, interfaces y usuarios administrativos.
- El licitante deberá considerar en su propuesta económica la capacidad de crear hasta 100 instancias de dispositivos virtuales (IPS virtuales) en todos los equipos ofertados.
- Para los equipos en el centro de datos principal se requiere una consola de Administración.

**4. Servicios de Protección contra Denegación (DDoS)**

| | Tipo 1 | Tipo 2 |
|---|---|---|
| Desempeño | 20 Gbps | 120 Gbps |
| Conexiones simultaneas por seg. | 25,000,000 | 120,000,000 |
| Conexiones nuevas por seg. | 160,000 | 600,000 |
| Interfaces 10GbE | 8 | 8 |

Se requieren mínimo 2 y máximo 4 equipos tipo 2 para el Centro de Datos Principal ubicado en Morelia Michoacán (configuración en HA)

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- El licitante deberá considerar en su propuesta que la cantidad de tráfico máximo a inspeccionar por lo equipos y un ancho de banda de los enlaces de internet que estarán recibiendo los equipos, de 1 Gbps para ambos casos.
- Deberá garantizar el paso transaccional de datos legítimos, privilegiando la eliminación de tráfico anómalo dentro de los canales de comunicación del Instituto (Clean Pipes).
- Detección del tráfico basado en el lenguaje TCPDUMP (con información definida en las capas 3 y 4)
- Deberá tener la capacidad de advertir anticipadamente algún posible ataque, analizando tendencias de tráfico malicioso en tiempo real.
- Deberá de tener capacidad de monitoreo en tiempo real de los circuitos dedicados que entregan la conectividad a Internet/Intranet para detectar el comportamiento anormal del tráfico que pueda estar dirigido a atacar las interfaces de los enrutadores implicados en los enlaces.
- Deberá de tener la capacidad de monitoreo en tiempo real las subredes pública que conectan los enlaces, para que permita la detección de tráfico anormal que pueda significar un ataque dirigida a ella.
- Detección de ataques basado en la línea de base contra los recursos definidos, con opciones configurables por recursos que permitan filtrar la sensibilidad de la anomalía y disparar un evento de tipo alerta, en paquetes por segundo y bytes por segundo.
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Capacidad de agrupar objetos tales como direcciones IP, protocolos y puertos para la simplificación de configuración de políticas de seguridad.
- Capacidad de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con tiempo de espera agotado (timeout).
- Deberá monitorear, de manera enunciativa más no limitativa, las siguientes variables en tiempo real:
    - Para el protocolo IP:
        - ICMP
        - Paquetes IP fragmentados
        - Paquetes IP NULL
        - Paquetes IP con direcciones privadas
    - Para el protocolo TCP:
        - Segmentos TCP NULL
        - Segmentos TCP RST

  - Segmentos SYN
  - Tráfico total
- Deberá como mínimo detectar los siguientes tipos de ataques DoS/DDoS sobre las interfaces, subredes y activos de infraestructura:
  - ACK Flood
  - SYN Flood
  - Hogging CPU
  - Chargen (Character generator)
  - FIN Flood
  - ToS Flood
  - DNS Malformed
  - HTTP Flood
  - ICMP Flood
  - UDP Flood
  - Non- UDP/TCP/ICMP Protocol Flood
  - PPS Flood Attack
  - Zombie attack
  - Land Attack
- Deberá de permitir la personalización de los niveles de alarma o umbrales que sirvan para la detección de ataques, a una granularidad por objeto monitoreado.
- Deberá monitorear actividad sospechosa que pueda significar algún ataque de gusanos, virus, entre otros.
- Deberá monitorear actividad "Dark IP".
- Detección de anomalías DDoS y amenazas de día cero antes de que impacten en los servicios.
- Detección de zombis (con selecciones de umbrales en bytes por segundos y paquetes por segundos) para clasificar una IP como zombis y con la opción de conocer una lista de zombis activos detectados.
- Protección contra amenazas conocidas
  - Ping de la muerte
  - Ataque por inundación SYN
  - Fragmentacion de paquetes y reensamblaje
  - Broadcast de correo electrónico
  - Saturadores de CPU
  - Scripts generadores de trafico
  - Generadores de caracteres
  - Ataques fuera de banda (WinNuke)
  - Ataque Smurf (generador de gran cantidad de paquetes ICMP)
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

**5. Redes Privadas Virtuales – VPN (C2S – S2S)**

Se requieren mínimo 1 y máximo 2 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuración en HA)

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Deberá incluir al menos 4 interfaces 10/100/1000 Gb, expandibles a interfaces 10Gb de ser necesario.
- Deberá tener un desempeño de al menos 2Gbps y 1,000,000 conexiones concurrentes
- Capacidad de permitir 50,000 nuevas conexiones por segundo.
- Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Deberá permitir implementar reglas aplicadas a intervalos de tiempo específicos.
- Deberá soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Deberá integrar esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Deberá permitir la creación de grupos de usuarios.
- Deberá permitir delimitar la cantidad de conexiones por usuarios.
- Deberá permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un servicio de autenticación externo.
- Capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
- Deberá soportar DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKEv2.
- Deberá soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Deberá soportar integridad de datos con md5, sha1 y sha2.
- Deberá soportar las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Deberá establecer VPNs con gateways con direcciones IP dinámicas públicas.
- Deberá crear una única asociación de seguridad (SA) por par de redes o subredes.
- Deberá realizar VPNs SSL.
- Deberá soportar la conexión desde dispositivos móviles y de escritorio a través de un cliente de acceso remoto. Dicho cliente debe soportar al menos las siguientes plataformas operativas: MAC OS X desde v10.4.10, iOS desde v4, Android desde v4.2, Windows desde v7.

**6. Filtrado de Contenido Web**

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Soportar de forma mínima 120,000 usuarios de forma simultánea.
- Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Permitir operar en modo de proxy explicito y/o proxy transparente.
- Mecanismos de autenticación tales como: archivos locales de contraseña NTLM, LDAP, RADIUS, Active Directory y certificados.
- Control de autenticaciones simultáneas con una misma cuenta de usuario.
- Cifrado de datos (usuario/contraseña) en el proceso de autenticación.
- Controlar e inspeccionar al menos los protocolos: HTTP, HTTPS (SSL), FTP, CIFS, MAPI, DNS, P2P, SOCKS (v4/v5), IM (AOL, MSN, Yahoo Messengers), TCP-Tunnel, MMS, RTSP.
- Catalogar las páginas por dominio (o subdominio), URL o IP.
- Bloqueo de las amenazas emergentes más comunes como: pop-ups, banners, spyware, adware, compartición de archivos punto a punto (P2P file sharing).
- Clasificación en tiempo real de sitios en internet (on-the-fly) que aún no han sido asignados a alguna categoría (servicio automático de validación en línea del sitio para determinar si es malicioso en caso de no tenerlo asignado en alguna categoría).
- Monitoreo y bloqueo de aplicaciones P2P tales como: BitTorrent, eDonkey, Gnutella, Fasttrack.
- Permitir personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
- Permitir la clasificación de URL (dominio o subdominio) o IP en una sola categoría.
- Permitir el uso de expresiones regulares.
- Permitir la creación de categorías de filtrado personalizadas, así como la creación de listas blancas y negras de filtrado URL.
- Capacidad de evitar la ejecución de códigos maliciosos.
- Bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.
- Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).
- Permitir la recopilación (caching) de páginas web en disco duro y memoria RAM, con el fin de hacer más eficiente el uso de los recursos del equipo.
- Proporcionar capacidades de administración y reporteo centralizado incluyendo control de acceso discrecional, control de versiones, auditoria de usuario, sistema y utilerías de restauración de configuración.
- Deberá proporcionar soporte de administración multisesión (múltiples administradores utilizando el servicio de administración centralizado), a través de una interfaz gráfica vía Web cifrada (HTTPS).
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre

otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.

**7. Servicios de Filtrado de Contenido de Correo (Antispam)**

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Capacidad de hasta 1.5M de correos por hora
- Con una capacidad de por lo menos 120,000 usuarios
- 12 TB por equipo, en HA por lo menos 24 TB.
- Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Capacidad de revisar tanto el correo entrante como el saliente.
- Deberá escanear y analizar el asunto, encabezados y el cuerpo de los correos recibidos y enviados.
- Contar con un filtro de contenido para buscar palabras clave en el cuerpo del mensaje, en los encabezados From, To, CC, Subject y en X-Headers. Así mismo, deberá poder detectar estas palabras en archivos adjuntos.
- Capacidad para poder configurar el tamaño máximo del mensaje y el número de destinatarios del correo tanto a nivel de conexión SMTP, como en políticas cuando el correo ya ha sido recibido.
- Contar con mecanismos para clasificar los remitentes por su origen y tomar decisiones de flujo y volumen en consecuencia. Además, se debe contar con la facilidad de designar ciertas fuentes de correo en grupos como listas negras, listas blancas o cualquier otro grupo al que deba aplicársele una política específica.
- Capacidad para ofrecer el análisis de archivos comprimidos en los formatos más populares, incluyendo aquellos con 7 capas de compresión.
- Capacidad de detectar el verdadero formato de un archivo y permitir aplicar políticas basadas en este rubro.
- Capacidad para detectar enlaces maliciosos dentro de los correos recibidos en base a la reputación de la URL, utilizando la tecnología de reputación del fabricante, permitiendo la configuración de umbrales para esta detección.
- Contar con un módulo de bloqueo de correo electrónico no deseado con base en la reputación de cuentas de correo, dominios y direcciones IP.
- Capacidad para soportar la revisión de firmas DKIM en los encabezados de correos entrantes.
- Contar con actualizaciones para sus patrones y motores de detección de spam (heurística), phising y código malicioso.
- Capacidades de colaboración con los centros de investigación de amenazas del fabricante, con la finalidad de reportar de manera automática cualquier comportamiento sospechoso relacionado con el tráfico de correo electrónico.
- Capaz de recibir tráfico con conexiones seguras (TLS) y poder hacer conexiones con otros servidores bajo el mismo protocolo.
- Contar con mecanismos que permitan evitar la recepción de correos de notificaciones dirigidas a cuentas de usuarios no válidos o que no existen en el dominio destino (correos de rebote o Bounced Mails).

- Bloqueo automático de IP debido a alta cantidad de envío de spam, ataque tipo DHA (Directory Harvest Attack), Bounced Mails o código malicioso, totalmente parametrizable al número de mensajes recibidos en un intervalo de tiempo determinado a discreción.
- Capacidad para Integrar excepciones, tanto en hosts remitentes como en destinatarios, así como para cuentas de usuarios o dominios específicos.
- Permitir la creación de cuarentenas o carpetas de auditoría de correo, la cuarentena debe poder ser almacenada por la solución como mínimo 30 días.
- Cuando se encuentre contenido malicioso en cuerpo del correo y archivos adjuntos, podrá realizar cualquiera de las siguientes acciones:
    - Reemplazar texto del mensaje afectado.
    - Poner en cuarentena el mensaje completo.
    - Eliminar el mensaje completo.
    - Hacer copia de seguridad (copia del mensaje), para reportarlo con los centros de investigación de amenazas del fabricante.
- Detectar correos masivos con virus y removerlos además de los archivos adjuntos, incluyendo la característica de archivos adjuntos Zero-byte.
- Proporcionar la facilidad de enviar notificaciones a los usuarios (cuentas de correo electrónico) cuando algún evento sospechoso sea detectado.
- Capacidad de integrar agentes que realicen la función de escaneo y detección de spam en activos de infraestructura o servicios de correo electrónico bajo plataformas operativas Linux y/o Windows.
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

**8. Firewall Especializado en Servicios Web (WAF)**

Se requieren mínimo 1 y máximo 2 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuración en HA)

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Inspección y análisis de perfiles de comportamiento normal de usuarios para detectar y mitigar el uso anormal de aplicativos Web.
- Soportar un throughput de 5 Gbps en capa 7.
- Soportar 100,000 Transacciones por Segundo (TPS).
- El licitante ganador debe considerar en su propuesta en términos de transacciones por segundo de tráfico HTTPS requiriendo PFS/DH (Perfect Forward Secrecy/ Diffie-Hellman) al menos 60,000 tps
- Servicio de reputación para identificar y bloquear ataques automatizados y/o usuarios maliciosos.
- Detección de ataques por clientes automatizados y robots.
- Detección de URL rewriting u ofuscación del URL.
- Manejo de errores y reescritura de errores para aplicativos Web.
- Capacidad para soportar inspección del protocolo XML.
- Certificado por organismos de la industria como ICSA Labs o PCI.
- Actualización automática de firmas de prevención contra código malicioso.
- Parcheo sobre aplicativos Web contra vulnerabilidades nuevas o conocidas (parcheo virtual).
- Protección contra ataques/vulnerabilidades conocidas (OWASP), de manera enunciativa más no limitativa:
    - SQL injection
    - Cross Site Scripting
    - Cross Site Request Forgery
    - Sensitive Data Exposure
    - Security Misconfiguration
    - Broken Authentication and Session Management
    - Otras nuevas identificadas por OWASP
- Soportar formatos de mensaje:
    - Web 2.0
    - HTML
    - XHML
    - HTML5
    - XML
    - JSON
    - AJAX
    - FLASH

- JavaScript.
- Soportar Protocolos: TCP v4 y v6, HTTP, HTTPS, SSL/TLS.
- Soportar mitigación de amenazas:
  - HTML Content Aware
  - Intrusion Detection and Prevention (URI patterns)
  - URI rate-based heuristics
  - Vendor Vulnerabilities
  - URL cloaking / rewrite
  - Parameter Inspection
  - Learning mode
- Integridad de transacciones:
  - Session Tracking Cookies, Source/Destination IPs
  - HTTP RFC conformance
  - HTML Form parameter checking
  - Cross-Site Scripting
  - Cookie Signing
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Debe soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
- El licitante deberá considerar en su propuesta al menos 200 sitios/portales a proteger.

**9. Servicios de Gestión Unificada de Amenazas (UTM)**

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

| | Tipo 1 | Tipo 2 | Tipo 3 | Tipo 4 |
|---|---|---|---|---|
| Desempeño | 1 Gbps | 2 Gbps | 5 Gbps | 10 Gbps |
| Conexiones simultaneas por seg. | 10,000 | 20,000 | 50,000 | 100,000 |
| Conexiones nuevas por seg. | 150,000 | 500,000 | 1,000,000 | 2,000,000 |
| Interfaces 10/100/1000 Mbps. | 4 | 4 | 8 | 8 |

Se requieren mínimo 1 y máximo 2 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuración en HA)

El licitante deberá considerar en su propuesta que funcionalidad de alta disponibilidad modo Activo/activo y/o Activo/Pasivo.

El licitante deberá considerar en su propuesta que la característica de conexiones simultaneas por segundo" y "conexiones nuevas por segundo, se refiera a conexiones concurrentes por segundo, así así como considerar que la suma de las sesiones concurrentes refiere a el servicio UTM por cada tipo y las sesiones concurrentes de la tabla de UTM.

Generales

- Deberá incluir un sistema operativo endurecido propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.

Funcionalidad Firewall

- Deberá estar basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
- Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Deberá permitir implementar reglas aplicadas a intervalos de tiempo específicos.
- Deberá soportar y operar bajo protocolos de ruteo BGP y OSPF.
- Deberá soporte y operar mediante rutas estáticas.
- Deberá realizar inspección en capa 3 y 4.

Funcionalidad IPS e IDS

- Soporte de al menos: 1,000,000 conexiones simultáneas por cada Gigabit de inspección.
- Latencia máxima de 0.5 milisegundos.
- Las interfaces de Inspección deberán operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
- El equipo deberá ser capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado
- Capacidad de detección en línea sin bloquear tráfico (Modo transparente). El sistema sólo alertará que eventos serían bloqueados.
- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.
- Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
- Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.
- La solución de IPS deberá contemplar que el flujo de información esté asegurado ante una falla en el IPS, pudiendo conmutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.
- Reconocimiento de tuneleo de protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
- Detección de re-ensamblaje de paquetes fragmentados.
- integración de listas blanca (IP whitelist) mediante una lista de direcciones IP "confiables" que el sistema no bloqueará.

- Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos hosts de la red y crear una alarma cuando cierto umbral sea rebasado.

Filtrado de Contenido Web

- Deberá permitir operar en modo de proxy explicito y/o proxy transparente.
- Controlar e inspeccionar al menos los protocolos: HTTP, HTTPS (SSL).
- Catalogar las páginas por Dominio (o subdominio), URL o IP.
- Permitir personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
- Permitir la creación de categorías de filtrado personalizadas, así como la creación de listas blancas y negras de filtrado URL.
- Capacidad de evitar la ejecución de códigos maliciosos.
- Permitir el bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.
- Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).

Funcionalidad VPN

- Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Deberá permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
- Deberá soportar DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKE v2.
- Deberá soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Deberá soportar integridad de datos con md5, sha1 y sha2.
- Deberá soportar las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Deberá establecer VPNs con gateways con direcciones IP dinámicas públicas.
- Deberá crear una única asociación de seguridad (SA) por par de redes o subredes.
- Deberá soportar Secure Sockets Layer (SSL) versión 3, con al menos los siguientes algoritmos de cifrado simétrico y longitud de llaves: RC4 (128 bits) y 3DES (192bits).

**10. Firewall Especializado en Base de Datos (DBF)**

Se requieren mínimo 1 y máximo 2 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuraciones en HA)

Especificaciones Técnicas:

- Tecnología de autoaprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo schemas, objetos, tablas; sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario.
- Deberá operar a nivel local y en la capa de red
- Deberá soportar al menos los siguientes motores de Bases de Datos:
  - Microsoft SQL Server
  - Oracle
  - Sybase
  - Informix
  - MySQL
  - Progress
  - PostgreSQL
- Proporcionar protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.
- En caso de ser necesario la utilización de agentes, estos deberán soportar al menos los siguientes Sistemas Operativos:
  - AIX
  - HP-UX
  - Solaris
  - RHEL
  - SusE
  - OEL
  - Windows 32/64 bits
- Capacidad para funcionar independiente a la activación de la auditoría nativa de la base de datos.
- Transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
- Se requiere un repositorio para el registro de la actividad, el cual no deberá ser accesible por ningún otro mecanismo que no sea la interacción mediante la GUI (interfaz gráfica) proporcionada por el fabricante o por medios administrativos debidamente asegurados.
- Capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de comunicación, y configuración de seguridad, sin importar el sistema operativo sobre el que se encuentren instaladas.
- Capacidad para poder realizar descubrimientos automatizados en la red para identificar nuevas bases de datos siendo habilitadas, ya sea a nivel de servidor o puertos habilitados en servidores conocidos.
- Capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo a las políticas de negocio. Las definiciones de tipo de dato deberán poder crearse de manera flexible y granular.

- Capacidad para proveer un servicio de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.
- Deberá apoyar en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y Control de cambios.
- Deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
- Deberá monitorear e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, ligas, stored procedures, entre otros.
- Deberá hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.
- Capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.
- Capacidad para proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.
- Deberá manejar reglas y políticas tan amplias o granulares como se requieran y deberán poder ser construidas automática o manualmente y deberán poder ser actualizadas, igualmente, de forma manual o automática.
- Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:
    - Número de registros a regresar por la consulta (SQL Query)
    - Número de registros afectados
    - Tipo de datos accesado (financiero, recursos humanos, inventarios, o cualquier definición personalizada)
    - Acceso a datos marcados como sensibles
    - Base de Datos, Schema, Instancia, Tabla y Columna accesada
    - Estado de autenticación de la sesión
    - Usuario y/o Grupo de Usuarios de Base de Datos conectado
    - Usuario conectado en la capa aplicativa, a diferencia del usuario conectado a la DB
    - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier customización por expresiones regulares)
    - Logins, Logouts, Queries
    - IPs de origen y destino
    - Nombre de Host origen, Usuario firmado en el Host origen
    - Aplicación usada para la conexión a la base de datos
    - Tiempo de respuesta/procesamiento del query
    - Errores en el manejador de SQL
    - Número de ocurrencias en intervalos de tiempo definidos
    - Por operaciones básicas (Select, Insert, Update, Delete)
    - Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export)
    - Por Stored Procedure o Function utilizada
    - Si existe ticket asignado de cambios
    - Hora del Día
- Deberá posibilitar los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.
- Deberá proteger contra ataques SQL y no-SQL.

- Contar con un mecanismo de actualización de la inteligencia interna de seguridad, que incluye las pruebas de las evaluaciones de vulnerabilidad, las firmas contra ataques, la granularidad de las políticas de seguridad y defensas contra comportamientos conocidos.
- Considerar de emergencia, para potenciales violaciones de la información que incluyan, enunciativa más no limitativamente:
  - Altos volúmenes de acceso a datos sensibles más allá de lo habitual.
  - Acceso a datos inusual para cierta hora del día.
  - Acceso a datos desde una ubicación (física) desconocida.
  - Acceso a datos utilizando aplicaciones/herramientas no autorizadas.
- Debe manejar una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.
- Debe tener facilidades de Archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP)
- Deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.
- Deberá contar con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de las mismas.
- Deberá soportar y aplicar simultáneamente un modelo de seguridad positivo y negativo.
- El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que deberá además cumplir con las siguientes especificaciones:
  - Deberá bloquear las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
  - Deberá incluir una lista pre-configurada y detallada de las firmas de ataque.
  - Deberá permitir la modificación o adición de firmas por el administrador.
  - Deberá permitir la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
  - Deberá detectar ataques conocidos a nivel base de datos
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Debe soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).

**11. Servicio de Correlación de Eventos**

Se requieren mínimo 2 y máximo 4 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuraciones en HA)

Especificaciones Técnicas:

- Capacidad para recolectar datos de toda aplicación o dispositivo que tenga una fuente de eventos necesaria para la organización, siendo esto a través de desarrollos predefinidos del fabricante, o con desarrollos personalizados ejecutados por el proveedor del servicio.
- Capacidad para almacenar la información tal y como fue recibida del dispositivo o aplicaciones (eventos en crudo), para efectos de auditoría y análisis forense. La solución deberá generar una

firma o "checksum" de los eventos recibidos para garantizar la integridad y mantener la cadena de custodia.

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

**12. Servicio de Protección de Amenazas Persistentes Avanzadas (APT)**

Se requieren mínimo 2 y máximo 4 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuraciones en HA)

Especificaciones Técnicas:

- Detectar cuando un equipo intenta hacer comunicación con un servidor de comando y control en Internet.
- Detectar cuando una amenaza intenta ingresar en la organización mediante internet.

- Detectar e interactuar cuando un atacante o código maliciosos está realizando actividades de movimientos laterales en la organización.
- Detectar ataques del tipo "zero day" que puedan intentar comprometer activos de la organización.
- Tener las capacidades de detección de anomalías en los puntos de la red designados, dicha detección no debe basarse en firmas ni heurística.
- Tener la capacidad de actuar no solo por la generación de alertas de los componentes tecnológicos implementados, si no capacidades de caza de amenazas.
- Contar con las capacidades de análisis y perfilamiento de los actores detrás de un ataque sobre el Instituto.
- Apoyará al Instituto en la detección y prevención de ataques avanzados, así como el manejo de los incidentes que deriven de ello.
- Elevar el nivel de visibilidad respecto a detección de amenazas avanzadas persistentes.
- Elevar el nivel de capacidades de actuación ante una amenaza avanzada persistente.
- Permitir contar con la información suficiente para identificar el impacto real de una amenaza.
- Permitir proteger diversos segmentos de la red del Instituto con diferentes niveles de protección de acuerdo con la criticidad de los usuarios de cada segmento.
- Permitir tener arquitectura modular y escalable de protección y viabilidad.
- Contar con un servicio especializado que permita apoyar al Instituto en la actuación y respuesta ante un ataque desarrollado con amenazas avanzadas.
- Acortar los tiempos de detección y actuación ante una amenaza avanzada.
- Integrar las capacidades de identificar una amenaza cuando tiene comunicación al exterior mediante el servicio de internet del Instituto o movimiento laterales en las diversas localidades, estas capacidades de detección deberán tener la capacidad de perfilar el comportamiento de los usuarios y sus dispositivos con el propósito de detectar cualquier anomalía que puede representar un impacto o riesgo para la Institución
- Disponer de una capa de inteligencia provista por los fabricantes de los componentes tecnológicos y fortalecida por la capa de inteligencia propia del Proveedor; dichas capas deben incluir al menos las siguientes características:
    - IP, URL Maliciosos
    - Hashes de archivos maliciosos
    - Tácticas, técnicas y procedimientos de los atacantes de la región en organizaciones similares al Instituto.
- Proporcionar las capacidades de realizar investigaciones en profundidad para detectar intrusiones que han pasado desapercibidas para los controles de seguridad implementados, esta investigación debe permitir al menos las siguientes capacidades:
    - Caza de amenazas que han estado activas, pero por su comportamiento no han podido ser detectadas.
    - Interacción con el código malicioso y ataques mediante la implementación de trampas en la red y la emulación de servicios.
    - Engaño de los atacantes mediante la implementación de información que pueda rastrear el origen de un ataque.
    - Análisis dinámico de los artefactos detectados.
    - Análisis de indicadores de compromiso en la red de cómputo del Instituto.
- Generar inteligencia accionable con la cual se puedan alimentar los controles preventivos para evitar que una amenaza conocida pueda volver a presentarse o la detección y contención sea temprana.

## 13. Antivirus

Se requieren servicios para el centro de datos principal ubicado en Morelia Michoacán en HA

Especificaciones Técnicas:

La solución propuesta por el proveedor deberá contar con las siguientes funcionalidades:

- La solución antivirus debe proteger a los siguientes sistemas operativos, en las plataformas Intel y AMD (Windows Server 2012 y posteriores).
- La solución antivirus deberá integrar agentes para la detección de virus, malware, entre otros en las plataformas de correo electrónico institucional (Exchange Server 2010 y superiores)
- Reputación Web
  - La solución de antivirus deberá contar con un sistema basado en la reputación de sitios web que permitan de manera proactiva evitar que los usuarios cuando naveguen descarguen componentes maliciosos e infecten sus estaciones de trabajo.
  - El sistema de reputación de archivos debe estar integrado o desagregado de la consola de antimalware.
  - Niveles de seguridad para evitar la navegación Web a sitios maliciosos cuando los usuarios se encuentran dentro o fuera de la red corporativa.
  - Permitir reclasificar sitios web.
  - El sistema de protección Web no deberá depender de ningún explorador en específico.
  - Permitir editar la lista de URL permitidas a nivel general, grupos o personal.
- Ataques de día Zero
  - Cuando es publicada o descubierta una vulnerabilidad en sistema operativo o en alguna aplicación, el Antimalware deberá ser capaz de detener un ataque causado por un malware que aprovecha la vulnerabilidad descubierta.
- Protección Antimalware
  - Detectar, analizar y eliminar programas maliciosos, como virus, spyware, gusanos, troyanos, keyloggers, programas publicitarios, rootkits, phishing, entre otros.
  - Detectar, analizar y eliminar, de forma automática y en tiempo real, los programas maliciosos en:
    - Procesos que se ejecutan en la memoria principal (RAM);
    - Archivos creados, copiar, renombrar, mover o modificados, incluyendo periodos de sesiones en la línea de comandos (DOS o shell) abiertos por el usuario;
    - Archivos comprimidos de forma automática, al menos en los siguientes formatos: ZIP, EXE, ARJ, MIME / UU, CAB de Microsoft, Microsoft Comprimir.
    - Archivos recibidos a través de software de comunicación instantánea (Whatsapp, MSN Messenger, Yahoo Messenger, Google Talk, ICQ, entre otros).
  - Detectar y proteger a la estación de trabajo contra acciones maliciosas que se ejecutan en navegadores Web mediante secuencias de comandos en lenguajes tales como JavaScript, VBScript / ActiveX, etc.
  - La detección heurística de virus desconocidos.
- Control de dispositivos
  - Proporcionar o restringir el acceso a dispositivos USB, Floppy, CD´s y Carpetas compartidas.

- La solución Antimalware deberá evitar una infección provocada por la ejecución del archivo Autorun.inf contenido en un dispositivo de USB al momento de ser conectado en la estación de trabajo.
- Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware deberá permitir al usuario hacer modificaciones, control total, solo lectura y ejecución, solo lectura en el contenido del dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger.

• Protección por comportamiento
  - Para aquellos programas que no están permitidos ser ejecutados en la estación de trabajo, deberán ser agregados a una lista de bloqueo de programas específicos.
  - Evitar o monitorear que un programa con comportamiento sospechoso pueda realizar lo siguiente:
    - Duplicar o inyectar archivos de sistema similares.
    - Modificar el archivo de HOST.
    - Incrustar elementos "plugins" en el navegador de Internet Explorer.
    - Instalar librería del programa malicioso.
    - Instale nuevos servicios.
    - Modifique archivos de sistema.
    - Instale servicios o programas para iniciarse al arrancar la estación de trabajo.
• Reporte de amenazas a los laboratorios
  - Capacidad de reportar eventos de amenazas aún no identificadas, de manera automática a través del comportamiento, a los laboratorios de antimalware para el análisis e identificación de la fuente y generación de una protección proactiva.
  - Capacidad de limitar los recursos utilizados para la notificación a los laboratorios, respetando la confidencialidad de la información.
  - Lanzar una política de seguridad en caso de epidemias.
• Métodos de Actualización, Instalación y desinstalación
  - Instalación de cliente antivirus mediante la URL de la Consola de la solución.
  - Instalación de cliente antivirus mediante línea de comandos o script.
  - Lanzamiento de instalación vía navegación de los grupos de trabajo de Windows.
  - Lanzamiento de instalación vía integración con el dominio de Active Directory.
  - Lanzamiento de instalación vía escaneo de equipos dentro de un segmento de Red.
  - Desinstalación del cliente desde el administrador de programas de Windows o el acceso directo a Uninstall.exe del menú inicio.
  - Desinstalación del cliente de forma remota desde la consola de administración.
  - Configuración de Actualizaciones automáticas, así como la fuente de actualización.
  - Distribución de actualizaciones a los clientes de manera Automática y Manual.
  - Actualización de sistema de firmas para clientes sin conectividad al servidor.
  - Actualización de grupo de usuarios por Agentes de Actualización o repositorios.
• Configuración de escaneos
  - Personalización de opciones de escaneo y Acción para una detección en los modos: Manual, en Tiempo Real y Programado.
• Privilegios de los usuarios
  - Personalizar los permisos de los clientes para realizar acciones en el software local.
  - Inhabilitación de los servicios y/o componentes del Cliente antivirus por medio de contraseña.
  - Habilitar o deshabilitar opciones para el cliente que frecuentemente entra/sale de la red local.

## 14. Servicios de Prevención de Perdida de Información

Se requieren servicios para el centro de datos principal ubicado en Morelia Michoacán en HA

Especificaciones Técnicas:

La solución propuesta por el proveedor deberá contar con las siguientes funcionalidades:

- Presente un Log de auditoría de todas las actividades de los usuarios.
- Proporcione Reportes predefinidos y personalizados que puedan ser programados o de una sola vez.
- Proporcione un mecanismo de alertas y notificaciones.
- Que sea capaz de proporcionar administración basada en roles múltiples con las siguientes opciones:
  - Capacidad para definir roles de usuarios tales como Administrador, administrador de la seguridad o administrador de cuentas.
  - Capacidad para agregar y modificar roles personalizados.
  - Capacidad de configurar cuentas de usuario y asignar un rol particular a cada usuario.
- Tecnología de Detección.
  - Capacidad para extraer textos de diferentes tipos de documentos para ejecutar escaneos de contenido.
  - Capacidad de realizar detecciones basadas en palabras (keywords) personalizadas o frases (key phrases) personalizadas, con la habilidad de poner diferentes palabras en una sola regla de detección.
  - Capacidad de detección basada en expresiones regulares.
  - Capacidad de detección basada en atributos de archivos tales como tipo de archivo y tamaño de archivo.
  - Capacidad de utilizar validación de reglas de expresión.
  - Capaz de extraer y ejecutar escaneo de contenido de documentos dentro de archivos comprimidos tales como archivos zip y rar.
  - Capaz de controlar la cantidad de capas de compresión que va a descomprimir en archivos comprimidos.
  - Capaz de soportar texto en diferentes idiomas (al menos español e inglés).
  - Que sea capaz de definir identificadores de datos a través de palabras, expresiones o atributos de archivos.
  - Proporcione identificadores de datos predefinidos.
  - Capaz de duplicar y personalizar identificadores de datos predefinidos y personalizados.
  - Capaz de crear identificadores de datos múltiples.
  - Que sea capaz de combinar palabras, expresiones y atributos de archivos dentro de plantillas para identificar información sensible.
  - Proporcione plantillas predefinidas.
  - Con capacidad para importar y exportar plantillas.
  - Capacidad para crear diversas plantillas personalizadas.
  - Capaz de combinar diversas plantillas dentro de una política.
  - Capacidad de crear diversas políticas.
  - Capacidad de crear políticas desde la consola de administración centralizada.
  - Capaz de soportar diversas acciones para una política simple.

- Capaz de definir un set diferente de acciones basado en la condición de la máquina si está dentro o fuera de la red.
- Capaz de soportar las siguientes acciones cuando haya fuga de información sensible:
  - Sólo registro del evento (Log violation only).
  - Bloqueo de la transferencia de datos (Block data transfer).
  - Alertas en el equipo del cliente (Client-side alerts).
  - Alertas en el servidor de DLP (Server-side alerting).
  - Almacenamiento de información para análisis forense (Forensic data-capture)

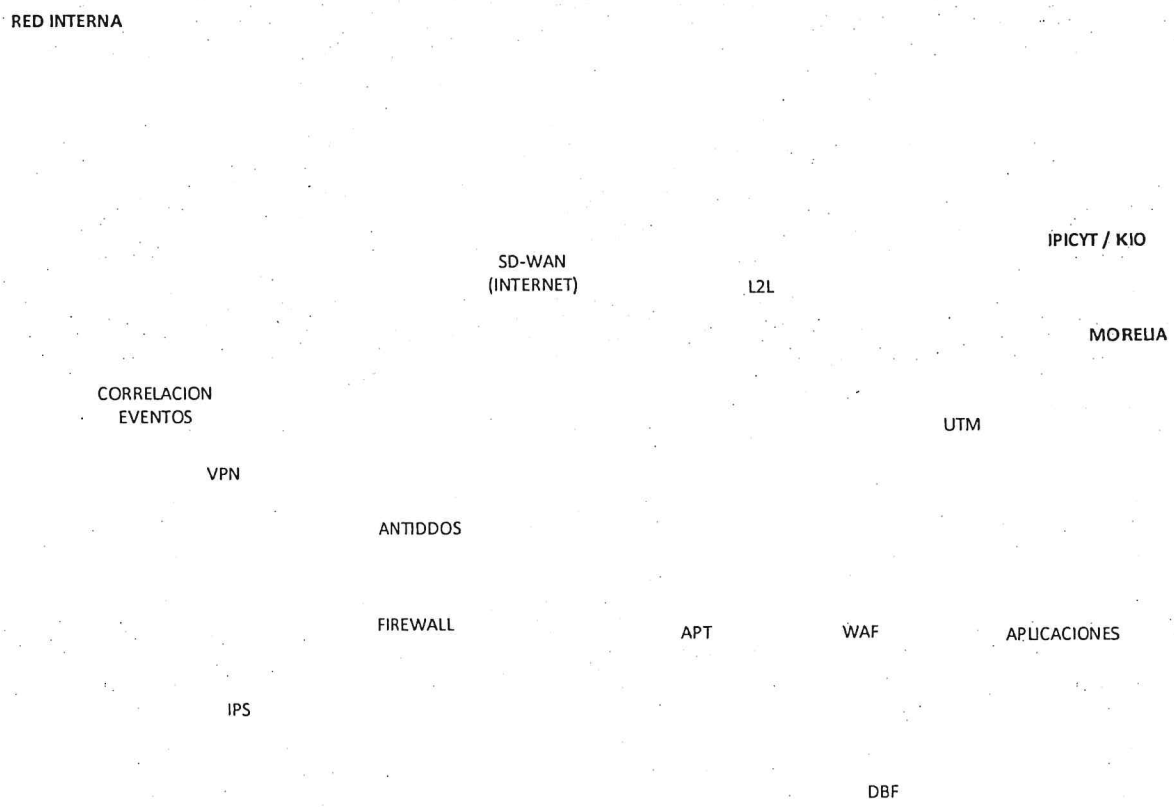
- Debe de ser capaz de ejecutar escaneos de contenido en los siguientes canales de información:
  - Correo electrónico
  - HTTP/HTTPS
  - FTP
  - Dispositivos removibles
  - Copia de información a CD/DVD
  - Mensajería instantánea
  - Comando de impresión
  - P2P
  - Portapapeles
  - Correo web
- Capaz de restringir acceso a los siguientes dispositivos:
  - Unidades extraíbles
  - Unidades ópticas
  - IEEE 1394
  - Impresión de pantalla
  - Bluetooth
  - Tarjetas PCMCIA
  - Carpetas compartidas
- Capaz de especificar excepciones de dispositivos
  - Capaz de definir diversas excepciones.
  - Capaz de utilizar comodines cuando se defina una excepción de dispositivos.
  - La configuración de control de dispositivos se debe de realizar de forma centralizada, desde la consola de administración.
  - Capaz de enviar un mensaje de notificación en la computadora del cliente.
  - Capaz de guardar en el log los eventos de control de dispositivos.

**15. Generales para todas las soluciones**

- Todas las soluciones deben de cumplir como mínimo con estas especificaciones y capacidades, lo cual son enunciativas más no limitativas.
- Las propuestas deberán considerar todos los componentes necesarios para su correcta operación (Equipo activo de Telecomunicaciones, cableado, módulos, etc.)
- Las propuestas Técnicas, deberán ser acompañadas de las hojas de especificaciones, trípticos y demás información que permita verificar el cumplimiento de las mismas.
- Los proveedores podrán realizar propuestas de mejora de cada una de las soluciones y/o diseño de la red con forme a sus propuestas. (Ver el diagrama 01 propuesta mínima esperada de las soluciones).

- De las propuestas de solución, podrán proponer arreglos tipo cluster.

DIAGRAMA 01. PROPUESTA MÍNIMA ESPERADA DE LAS SOLUCIONES




**16. Especificaciones físicas y estándares de conexión para los insumos que conforman los Servicios Administrados de Seguridad Informática 2022-2024**

- Especificación y requerimientos de energía eléctrica

El Instituto proporcionará las facilidades dentro de los centro de datos para la alimentación eléctrica (contactos regulados), para el funcionamiento y operación del equipamiento propuesto por el licitante, el proveedor deberá considerar en su propuesta técnica la característica, cantidad, ubicación y los tipos de contactos requeridos para el aprovisionamiento inicial.

- Especificación y requerimientos de espacio físico y ambiental

El Instituto proporcionará la información específica respecto al espacio físico asignado para que el proveedor adjudicado instale la infraestructura de redes y seguridad en los centro de datos correspondientes. Para tal efecto el licitante deberá incluir en su propuesta técnica un apartado indicando la cantidad de espacio físico mínimo indispensable que se requerirá para la instalación de la infraestructura de seguridad.

También se deberá contar con las facilidades para su instalación y se deberá apegar al reglamento y políticas internas para la instalación dentro de cada Centro de Datos. Así también deberá indicar las condiciones ambientales adecuadas para el funcionamiento del equipo a instalar para dar el servicio.

- Especificación y requerimiento para el montaje de hardware

Debido a que el requerimiento del Instituto es un servicio administrado, será responsabilidad del proveedor adjudicado el montaje de los equipos propuestos, racks, gabinetes, rack de panel de parcheo (Parch panel rack), distribuidores fibra óptica, y todo lo necesario para la correcta operación de la solución propuesta, por lo que, en su propuesta económica debe considerar todo lo necesario con la finalidad de proveer lo necesario.

- Especificación para racks

El proveedor adjudicado deberá cumplir con las especificaciones de los racks y gabinetes, incluyendo sus dimensiones físicas, para cada uno de los centros de datos donde el Instituto indique para implementar los Servicios SASI 2022-2024, y en apego a las normas y estándares de la industria y los que se acuerdan o indiquen durante las mesas de trabajo con el Instituto.

- Políticas de cableado estructurado en centro de datos

El proveedor adjudicado deberá cumplir con los requerimientos para cada uno de los Centros de Datos donde el Instituto indique implementar los Servicios SASI 2022-2024, y en apego a las normas y estándares de la industria y los que se acuerdan o indiquen durante las mesas de trabajo con el Instituto, así mismo el proveedor adjudicado deberá suministrar los elementos para la interconectividad necesarios, por lo que deberá: proporcionar e implementar los distribuidores de fibras, las canaletas, los jumpers, y cualquier otro elemento que sea necesario para la correcta interconexión de los racks o puntos de interconexión bajo los estándares de cableado estructurado.

- Especificación de cableado para racks

El licitante deberá contemplar dentro de su propuesta (tanto para el aprovisionamiento inicial, como durante la operación y vigencia del contrato), todo el cableado, jumpers y patch cords necesarios para lograr la interconexión propuesta de todos y cada uno de los módulos y elementos del sistema.

- Especificaciones y requerimientos técnicos de cableado y conectores

Todos los componentes del sistema de cableado, así como troncales de cobre y/o fibra –excepto los correspondientes a los servidores- necesarios para la interconexión de todos los módulos de hardware solicitados para suministrar el servicio de SASI 2022-2024 en el Centro de Datos deberán incluirse como



DIVISIÓN DE CONTRATOS

2022 Año de Ricardo Flores Magón

parte de la propuesta de los Licitantes y deberán ser sin costo extra para el IMSS. Asimismo, en el caso de incrementos en los servicios deberán estar incluidos.

- Especificaciones y requerimientos técnicos de equipo de comunicaciones de red

Todos los componentes de interconexión (comunicaciones o balanceo de cargas) que apoyen la operación y administración que se lleve a cabo entre las soluciones de seguridad y red, que por su naturaleza sean requeridos para la puesta en operación del servicio de SASI 2022-2024 en el Centro de Datos, deberán incluirse como parte de la propuesta de los Licitantes y deberán ser sin costo extra para el IMSS. Asimismo, en el caso de incrementos en los servicios deberán estar incluidos.

- Políticas de seguridad de acceso físico a externos

El proveedor adjudicado deberá cumplir las políticas de seguridad de acceso físico a externos en los centros de datos donde el instituto determine para la provisión de los Servicios correspondientes SASI 2022-2024.

- Especificación y requerimientos de sistema de canalización.

El proveedor adjudicado deberá salvaguardar la integridad física del cableado para evitar fallas potenciales en la operación. De este modo, para salvaguardar la correcta operación del sistema de cableado de fibra óptica y cableado UTP, el licitante ganador utilizará la infraestructura existente en los Centros de Datos y, en general, cumplirá con las norma y políticas de canalización en los mencionados Centros de Datos.

**17. Condiciones para los servicios de mantenimiento**

El proveedor adjudicado será responsable de realizar las tareas de mantenimiento preventivo y correctivo para la totalidad de la infraestructura dentro del alcance de los servicios de SASI 2022-2024, a través de las labores que considere necesarias y de acuerdo con la estrategia de entrega y soporte de los servicios correspondientes. Enseguida se detallan las condiciones específicas para este servicio.

**18. Condiciones para los servicios de mantenimiento preventivo**

Como parte del Servicio de Mantenimiento el proveedor adjudicado deberá realizar al menos un mantenimiento preventivo al año a toda la infraestructura que forme parte del contrato de SASI 2022-2024. Para lo cual deberá integrar un Plan de Mantenimiento Preventivo, en el cual debe tomar en cuenta para la proyección de mantenimientos, las ventanas de mantenimiento necesarias, con el fin de ser programadas e informadas con anticipación al administrador del contrato, con objeto de minimizar el impacto a la operación.

En la correspondiente propuesta técnica el licitante, deberá incluir un Plan de Mantenimiento Preventivo, el cual deberá incluir como mínimo:

- La descripción de los procesos asociados.
- Los Recursos Humanos y Materiales involucrados.
- Los alcances técnicos del mantenimiento y los protocolos de prueba.
- Las rutas de escalamiento correspondientes.

Esta información debe agruparse por tipo de equipo o infraestructura. Para cada caso, el proveedor adjudicado deberá contemplar el calendario de los servicios de mantenimiento preventivo, el cual será validado y autorizado por administrador del contrato, quien revisará que no afecte períodos críticos de la operación del Instituto.

El calendario final de mantenimientos preventivos, fundamentado en el Plan de Mantenimiento Preventivo que se entregará durante las Mesas de Trabajo, será elaborado por El licitante ganador y autorizado por el Instituto, acotando los inmuebles, fechas y actividades a realizar con el máximo detalle, a efectos de coordinar todas las labores necesarias para su correcta ejecución.

**19. Condiciones para los servicios de mantenimiento correctivo**

El proveedor adjudicado será responsable de realizar el mantenimiento correctivo para los servicios correspondientes de SASI 2021-2024, para lo cual, previamente deberá integrar a su propuesta los procedimientos para reportar un incidente que requiera mantenimiento correctivo, y un ejemplo de matriz de escalamiento con los niveles y tiempos establecidos entre cada nivel.

Como parte de las Mesas de Trabajo, El licitante ganador deberá proporcionar la Matriz de Escalamiento con los nombres de contactos y responsables.

El licitante ganador efectuará el servicio de Mantenimiento Correctivo cuantas veces sea necesario durante la vigencia del servicio, de acuerdo con las especificaciones técnicas del fabricante y consistirá en la reparación o remplazo de las partes dañadas del equipo, cuando ocurra una falla que así lo requiera.

Si el equipo en cuestión no puede ser reparado, deberá sustituirse por otro equipo de características técnicas iguales o superiores, sin que esto implique la degradación del nivel de servicio requerido para dicho equipo. El tiempo para el reemplazo de partes no deberá exceder los 30 días naturales, durante los cuales El licitante ganador deberá proporcionar un equipo provisional para mantener la operación. El tiempo para el reemplazo de equipos no deberá exceder los 45 días naturales, durante los cuales el licitante ganador deberá proporcionar un equipo provisional para mantener la operación.

# Apéndice "B"

# Servicios Administrados de Seguridad Informática (SASI) 2022-2024

**Objetivo del Documento**

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

**2. Inventario de Activos de Infraestructura – Servicios de Continuidad**

| CONCEPTO | Sitio | Marca | Modelo | Número Serie |
|---|---|---|---|---|
| **I. Servicios de Seguridad - Continuidad Operativa** | | | | |
| 1. Arquitectura de Firewall. | | | | |
| Tipo 1 | IPICYT | Fortinet | FG-1100E | FG10E0TB21900070 |
| Tipo 2 | CENATI MONTERREY | Fortinet | FG-1100E | FG10E0TB21900374 |
| | CENATI MONTERREY | Fortinet | FG-1100E | FG10E0TB20903342 |
| Tipo 3 | CENATI MÉXICO | Fortinet | FG-1800F | FG180FTK20900846 |
| | CENATI MÉXICO | Fortinet | FG-1800F | FG180FTK20901096 |
| | JALISCO | Fortinet | FG-1800F | FG180FTK20900666 |
| | JALISCO | Fortinet | FG-1800F | FG180FTK20900667 |
| Tipo 4 | IPICYT | Fortinet | FG-4200F | FG420FTK20900121 |
| | IPICYT | Fortinet | FG-4200F | FG420FTK20900136 |
| 2. Prevención de Intrusiones (IPS) | | | | |
| Tipo 1 | CENATI MÉXICO | Fortinet | FG-1800F-BDL-950-12 | FG180FTK20901206 |
| Tipo 2 | CENATI MONTERREY | Fortinet | FG-2200E-BDL-950-12 | FG2K2ET920900397 |
| Tipo 3 | CENATI MÉXICO | Fortinet | FG-3300E-BDL-950-12 | FG3K3ET919900293 |
| | CENATI MÉXICO | Fortinet | FG-3300E-BDL-950-12 | FG3K3ET919900310 |
| Tipo 4 | IPICYT | Fortinet | FG-3300E-BDL-950-12 | FG3K3ET919900331 |
| | IPICYT | Fortinet | FG-3300E-BDL-950-12 | FG3K3ET919900323 |
| 3. Anti-denegación de servicios DDoS | | | | |
| Tipo 1 | CENATI MONTERREY | Fortinet | FDD-1500F | FI1K5FTE20000010 |
| | CENATI MONTERREY | Fortinet | FDD-1500F | FI1K5FTE20000039 |

| | | | | |
|---|---|---|---|---|
| Tipo 2 | IPICYT | Fortinet | FDD-1500F | FI1K5FTE20000009 |
| | IPICYT | Fortinet | FDD-1500F | FI1K5FTE20000045 |
| 4. Redes Privadas Virtuales (VPN) | | | | |
| | IPICYT | Fortinet | FG-1100E | FG10E0TB21900305 |
| | IPICYT | Fortinet | FG-1100E | FG10E0TB20903417 |
| | IPICYT | Fortinet | FG-1100E | FG10E0TB20903544 |
| | IPICYT | Fortinet | FG-1100E | FG10E0TB21900273 |
| 5. Filtrado de contenido web (WEBFILTERING) | | | | |
| | IPICYT | Fortinet | FG-1801F-BDL-950-12 | FG181FTK20900649 |
| | IPICYT | Fortinet | FG-1801F-BDL-950-12 | FG181FTK20900909 |
| | IPICYT | Fortinet | FG-1801F-BDL-950-12 | FG181FTK20901026 |
| | IPICYT | Fortinet | FG-1801F-BDL-950-12 | FG181FTK20901059 |
| 6. Antispam | | | | |
| | IPICYT | Fortinet | FML-3200E-BDL-641-12 | FE3K2ET319000024 |
| | IPICYT | Fortinet | FML-3200E-BDL-641-12 | FE3K2ET319000028 |
| | IPICYT | Fortinet | FML-3200E-BDL-641-12 | FE3K2ET319000029 |
| | IPICYT | Fortinet | FML-3200E-BDL-641-12 | FE3K2ET319000035 |
| 7. Firewall Especializado en Servicios Web (WAF) | | | | |
| | IPICYT | IMPERVA | X10K2 | 2030BA3322 |
| | IPICYT | IMPERVA | X10K2 | 2030BA3319 |
| | CENATI MONTERREY | IMPERVA | X10K2 | 2030BA4461 |
| | CENATI MONTERREY | IMPERVA | X10K2 | 2030BA4457 |
| 8. Firewall de Base de Datos (DBF) | | | | |
| | IPICYT | IMPERVA | X6520 | 2030BA3391 |
| | IPICYT | IMPERVA | X6520 | 2030BA3392 |
| | CENATI MONTERREY | IMPERVA | X6520 | 2113BA0235 |
| | CENATI MONTERREY | IMPERVA | X6520 | 2113BA0238 |
| 9. Gestión Unificada de Amenazas (UTM) | | | | |
| Tipo 1 | ATLIXCO | Fortinet | FG-100F-BDL-950-12 | FG100FTK21003654 |
| Tipo 2 | OAXTEPEC | Fortinet | FG-400E-BDL-950-12 | FG4H0ETB20902009 |

| | | | | |
|---|---|---|---|---|
| Tipo 3 | CENATI MONTERREY | Fortinet | FG-600E-BDL-950-12 | FG6H0ETB21901099 |
| Tipo 4 | CENATI MÉXICO | Fortinet | FG-1800F-BDL-950-12 | FG180FTK20901163 |

## Apéndice "B-bis"
## Servicios Administrados de Seguridad Informática (SASI) 2022-2024

### 1. Objetivo del Documento

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

### 2. Inventario de Activos de Infraestructura – Servicios de Continuidad

| No. | Descripción del servicio | Unidad de medida | Cantidad referencial mínima | Cantidad referencial máxima |
|---|---|---|---|---|
| 1 | Licenciamiento Firewall (Tipo 1) - Renovacion | Servicio | 1 | 1 |
| 2 | Licenciamiento Firewall (Tipo 2) - Renovación | Servicio | 2 | 2 |
| 3 | Licenciamiento Firewall (Tipo 3) - Renovación | Servicio | 4 | 4 |
| 4 | Licenciamiento Firewall (Tipo 4) - Renovación | Servicio | 2 | 2 |
| 5 | Licenciamiento IPS (Tipo 1) - Renovación | Servicio | 1 | 1 |
| 6 | Licenciamiento IPS (Tipo 2) - Renovación | Servicio | 1 | 1 |
| 7 | Licenciamiento IPS (Tipo 3) - Renovación | Servicio | 2 | 2 |
| 8 | Licenciamiento IPS (Tipo 4) - Renovación | Servicio | 2 | 2 |
| 9 | Licenciamiento Anti-denegación de servicios DDoS (Tipo 1) - Renovación | Servicio | 2 | 2 |
| 10 | Licenciamiento Anti-denegación de servicios DDoS (Tipo 2) - Renovación | Servicio | 2 | 2 |
| 11 | Licenciamiento Redes Privadas Virtuales - Renovación | Servicio | 4 | 4 |
| 12 | Licenciamiento Filtrado de Contenido Web - Renovación | Servicio | 4 | 4 |
| 13 | Licenciamiento Filtrado de Contenido de Correo (Antispam) - Renovación | Servicio | 4 | 4 |
| 14 | Licenciamiento Firewall Especializado en Servicios Web (WAF) - Renovación | Servicio | 4 | 4 |
| 15 | Licenciamiento Firewall Especializado en Base de Datos (DBF) - Renovación | Servicio | 4 | 4 |
| 16 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 1) - Renovación | Servicio | 1 | 1 |
| 17 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 2) - Renovación | Servicio | 1 | 1 |

| | | | | |
|---|---|---|---|---|
| 18 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 3) - Renovación | Servicio | 1 | 1 |
| 19 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 4) - Renovación | Servicio | 1 | 1 |

## Anexo 2.- Términos y Condiciones

### 1. Objetivo del documento

Establecer las necesidades y condiciones de entrega de los "Servicios Administrados de Seguridad Informática 2022-2024".

### 2. Premisa

Las bases de datos, aplicaciones y cualquier otro tipo de información utilizadas en el suministro de los servicios o a la que se tenga acceso derivado de la naturaleza de los servicios, que sean propiedad exclusiva del Instituto Mexicano del Seguro Social ("El Instituto") continuarán siendo propiedad exclusiva del mismo. En ese sentido, el proveedor se obliga a utilizarlas exclusivamente para cubrir los servicios requeridos.

El proveedor deberá presentar como parte de su propuesta técnica escrito firmado por su representante legal respecto de las obligaciones de confidencialidad, las cuales estarán sujetas a lo dispuesto por la Ley Federal de Transparencia y Acceso a la Información Pública o por la Ley correlativa aplicable al Instituto.

### 3. Nombre del proyecto

**"Servicios Administrados de Seguridad Informática 2022 – 2024"**

### 4. Objetivos del proyecto

El Instituto Mexicano del Seguro Social (IMSS), a través de la Dirección de Innovación y Desarrollo Tecnológico (DIDT) requiere contar de manera integrada y unificada, con los servicios administrados que brinden la continuidad operativa, de negocio y de seguridad de la información del Instituto que:

- Asegure y proteger la información Institucional.
- Garantice la continuidad operativa, de negocio y de la seguridad de la información de la Institución, durante la vigencia del presente contrato, especialmente durante la toma de operación y transición del contrato anterior a los servicios propios de SASI 2022-2024.
- Fortalezca la seguridad de la información de la Institución contra amenazas, disminuyendo el riesgo de sufrir incidentes de seguridad, mediante el uso de tecnología de punta para el monitoreo, detección, aseguramiento, contención y respuesta ante ataques que puedan presentarse en la infraestructura de cómputo, sistemas y aplicaciones del IMSS.
- Cuente con servicios de infraestructura regulados por niveles de servicio, que: implementen (instalen, migren, habiliten y pongan a punto) los componentes necesarios en los centros de datos y servicios propios del IMSS y que de forma complementaria gestionen (operen, monitoreen, den soporte y mantenimiento preventivo y correctivo) a la correspondiente infraestructura con el propósito de satisfacer las necesidades de: conectividad, comunicación, protección, control y filtrado de la propia Institución, manteniendo la plataforma tecnológica en condiciones óptimas de operación.
- Cuente con los servicios de protección de forma unificada e integrada, incluyendo prevención de pérdida de información, protección de cómputo físico o virtual, correo electrónico externo e interno,

herramientas de colaboración, acceso a internet e intranet, filtrado; mediante una solución integral que permita una gestión consolidada de las funcionalidades, características y servicios, con el propósito de mantener, asegurar y robustecer el esquema de seguridad del IMSS.

- Cuente con servicios de seguridad de la información, que complementen el esquema de seguridad institucional de forma consistente y robusta, con el control, aseguramiento, diagnóstico, pruebas, metodologías, de distintos rubros como el de acceso a cuentas privilegiadas, base de datos, aplicaciones, fuentes múltiples, vulnerabilidades, investigación forense y de procesos de seguridad, así como con otros servicios especializados en materia de seguridad y tecnologías de la información.
- Cuente co n servicios para la capacitación y de soporte extendido que tienen como objetivo coadyuvar en la prestación del resto de los servicios SASI 2022-2024.

**5. Normas oficiales o certificaciones**

- Certificado ISO/IEC27001:2013
- Ceritificado ISO/IEC20000-1:2018

Ambos vigentes a nombre del licitante participante.

**6. Folletos, catálogos, fotografías, manuales entre otros**

No aplica

**7. Visitas a las instalaciones**

No se requiere.

**8. Tipo de abastecimiento requerido**

El tipo de abastecimiento será mediante dos partidas.

**9. Garantías**

El proveedor, se obliga a constituir en la forma y términos previstos por los artículos 48 y 49 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 103 de su Reglamento y numerales 4.30 y 4.30.3 de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social, la garantía de cumplimiento divisible correspondiente.

En cualquier momento, el instituto podrá hacer válida la póliza de garantía del contrato en caso de que el proveedor no cumpla con los tiempos y plazos de entrega establecidos en los presentes Términos y Condiciones.

Las modificaciones a las fianzas deberán formalizarse con la participación que corresponda a la afianzadora, en términos de las disposiciones aplicables.

La garantía permanecerá vigente a partir de la fecha de adjudicación del contrato respectivo, y hasta que se cumplan plenamente todas y cada una de las obligaciones del contrato, así como durante la substanciación de todos los recursos legales o juicios que, en su caso, sean interpuestos por cualquiera de las partes y hasta que se dicte la resolución definitiva por autoridad competente.

Para garantizar el cumplimiento de todas y cada una de las obligaciones estipuladas en el contrato Adjudicado, el proveedor se compromete a entregar, dentro de los 10 (diez) días naturales posteriores a la firma del contrato correspondiente, de conformidad con el artículo 103 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, por el 10% del monto máximo por el que se adjudica el contrato, a favor de el instituto, el cual será un contrato abierto y la garantía será divisible.

El proveedor, se obliga a entregar a el Instituto la póliza de fianza antes señalada, en la división de contratos, ubicada en calle Durango número 291, piso 10, Colonia Roma Norte, Alcaldía Cuauhtémoc, apegándose al formato que para tal efecto se entregará en la referida División.

**a) Devolución de garantías**

La liberación de garantías relativas al cumplimiento del Contrato podrán realizarse una vez que haya transcurrido el plazo de garantía indicado, a solicitud expresa por el proveedor por escrito en papel membretado de su empresa, dicha solicitud debe dirigirse a la Coordinación de Adquisición de Bienes y Contratación de Servicios, quien autorizará la devolución o cancelación de la póliza de garantía (fianza) correspondiente, dicha autorización se entregará al proveedor, siempre que demuestre haber cumplido con la totalidad de las obligaciones adquiridas por virtud del presente Contrato.

La garantía de cumplimiento a las obligaciones del contrato únicamente podrá ser liberada mediante autorización expresa y por escrito otorgado por la División de Seguridad Informática Física.

**b) Ejecución de la garantía**

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.
- Se rescinda administrativamente el contrato.
- La ejecución de la garantía será con independencia de la aplicación de las penas convencionales que procedan y de la rescisión administrativa del contrato.
- La ejecución de la garantía de cumplimiento del contrato será proporcional al monto de las obligaciones incumplidas.
- Además de las sanciones anteriormente mencionadas, serán aplicables las que estipulen las disposiciones legales vigentes en la materia.

## 10. Acuerdos de Niveles de Servicio

El objetivo de los niveles de servicio consiste en proporcionar al Instituto un mecanismo que permita:

- Medir de forma efectiva el desempeño de los servicios proporcionados por el proveedor.
- Procurar que los servicios le sean proporcionados con la calidad prevista.

De conformidad con lo establecido en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el Instituto aplicará penas convencionales por el atraso en el cumplimiento de las fechas pactadas de entrega o de la prestación del servicio, las que no excederán del monto de la garantía de cumplimiento del contrato, y serán determinadas en función de los bienes o servicios no entregados o prestados oportunamente.

### 10.1. Penas Convencionales

Se aplicarán penas convencionales por incumplimiento en el plazo de prestación de los servicios por parte del proveedor adjudicado del 0.2% por cada día natural de atraso en el inicio de la prestación del servicio, respecto del valor máximo total del contrato.

### 10.2. Servicios de Habilitación, Operación y Transición

**Partida 1 y 2**

| DESCRIPCIÓN DEL NIVEL DE SERVICIO | FECHA DE ENTREGA | PENA CONVENCIONAL MENSUAL | FÓRMULA DE CÁLCULO |
|---|---|---|---|
| Plan de trabajo detallado de los servicios del proyecto | 15 días naturales posteriores a la emisión del fallo | 1% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Documento Compromiso de suscripción de OLAs | 15 días naturales posteriores a la emisión del fallo | 1% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Matriz de Escalación | 15 días naturales posteriores a la emisión del fallo | 1% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios | 15 días naturales posteriores a la emisión del fallo | 1% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

### 10.3. Servicios de Seguridad – Continuidad Operativa

## Partida 1

| DESCRIPCIÓN DEL NIVEL DE SERVICIO | FECHA DE ENTREGA | PENA CONVENCIONAL MENSUAL | FÓRMULA DE CÁLCULO |
|---|---|---|---|
| Documento con el diseño de alto nivel de las soluciones de seguridad a implementar en los centros de datos o donde lo indique el Instituto | 5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Documento con el diseño de bajo nivel de las soluciones de seguridad a implementar en los centros de datos o donde lo indique el Instituto | 10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Memorias técnicas iniciales de las soluciones de seguridad implementadas | 10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Memorias técnicas actualizadas de los servicios de seguridad | 20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

### 10.4. Servicios de Seguridad – Verificación/Calidad

**Partida 1**

| DESCRIPCIÓN DEL NIVEL DE SERVICIO | FECHA DE ENTREGA | PENA CONVENCIONAL MENSUAL | FÓRMULA DE CÁLCULO |
|---|---|---|---|
| Documento con el diseño de Alto Nivel de los servicios de Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integran activos de infraestructura para su habilitación | 5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto | 10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integran activos de infraestructura para su habilitación | 10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| DESCRIPCIÓN DEL NIVEL DE SERVICIO | FECHA DE ENTREGA | PENA CONVENCIONAL MENSUAL | FÓRMULA DE CÁLCULO |
|---|---|---|---|
| Memorias Técnicas Actualizadas de las Servicios de Seguridad que requieran integran activos de infraestructura para su habilitación | 20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| <u>Procedimientos de Operación del servicio</u><br>• Servicios de Borrado Seguro de Información<br>• Servicio de Gestión de Dominios<br>• Servicio de Certificados Digitales SSL<br>• Servicios de Ciberinteligencia<br>• Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos móviles<br>• Servicios de Antivirus<br>• Servicios de Prevención de Perdida de Información | 10 días hábiles posteriores a la integración de las mesas de trabajo | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Metodología de implementación de los servicios.<br>• Servicios de Sistema de Gestión de Seguridad de la | 10 días hábiles posteriores a la integración de las mesas de trabajo | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| DESCRIPCIÓN DEL NIVEL DE SERVICIO | FECHA DE ENTREGA | PENA CONVENCIONAL MENSUAL | FÓRMULA DE CÁLCULO |
|---|---|---|---|
| Información (SGSI)<br>• Servicios de Gestión del Cambio en Seguridad de la Información | | | |

**Partida 2**

| DESCRIPCIÓN DEL NIVEL DE SERVICIO | FECHA DE ENTREGA | PENA CONVENCIONAL MENSUAL | FÓRMULA DE CÁLCULO |
|---|---|---|---|
| <u>Procedimientos de Operación del servicio</u><br>• Servicio de Análisis de Vulnerabilidades Estático<br>• Servicio de Análisis de Vulnerabilidades Dinámico<br>• Servicios de Análisis Forense<br>• Servicio de Pruebas de Penetración | 10 días hábiles posteriores a la integración de las mesas de trabajo | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

**10.5. Servicios del Centro de Operaciones de Seguridad (SOC)**

**Partida 1**

| DESCRIPCIÓN DEL NIVEL DE SERVICIO | FECHA DE ENTREGA | PENA CONVENCIONAL MENSUAL | FÓRMULA DE CÁLCULO |
|---|---|---|---|
| Procesos de operación implementados:<br>• Requerimientos<br>• Cambios<br>• Configuraciones<br>• Incidentes<br>• Problemas<br>• Monitoreo | 15 días naturales posteriores a la emisión del fallo | 2% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Matriz de Escalación Técnica y Organizacional | 15 días naturales posteriores a la emisión del fallo | 2% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Procedimiento de operación de la Mesa de Servicios:<br>• Requerimientos<br>• Cambios<br>• Configuraciones<br>• Incidentes<br>• Problemas<br>• Monitoreo | 15 días naturales posteriores a la emisión del fallo | 2% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Expedientes Curriculares del personal del SOC | 15 días naturales posterior a la emisión del fallo | 2% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

### 10.6. Deducciones

Durante la vigencia del contrato, al presentarte una falla, incidente, atención de requerimientos, ventana de mantenimiento, entre otras, cuya causa raíz haya sido derivada por un tercero, la deductiva correspondiente al servicio asociado no será aplicada al proveedor de SASI 2022-2024, siempre y cuando demuestre con evidencias fehacientes que el servicio correspondiente se presentó bajo las especificaciones del anexo técnico, términos y condiciones y los apéndices A y B.

Con base en lo anterior, y cuando las fallas, incidentes, atención de requerimientos, ventanas de mantenimiento, entre otras, sean atribuibles a la entrega de los servicios de seguridad por parte del Proveedor, se aplicarán deductivas conforme lo siguiente rubros:

### 10.7. Disponibilidad

## Partida 1

La disponibilidad se define como la medida del porcentaje de tiempo, en que el sistema que brinda el servicio de seguridad de SASI 2022-2024, (o un componente del sistema) realiza la función que le es propia. Es decir; disponibilidad es la proporción de tiempo en que el sistema cumple con la función para la cual está dispuesto, en relación con el tiempo en que debería haber estado disponible.

Las mediciones de disponibilidad deberán ser realizadas por el Proveedor de SASI 2022-2024, usando su correspondiente herramienta de monitoreo del servicio y herramienta de gestión de incidentes, con el afán de obtener mediciones precisas con respecto a los tiempos operacionales y los no operacionales y sus atribuibles.

Deberán realizarse mediciones de disponibilidad desde el inicio del período operacional de los servicios de infraestructura SASI 2022-2024, para todos los módulos o posiciones de servicio contratados.

El Proveedor de SASI 2022-2024, comprometerá la disponibilidad en base a los siguientes factores:

Incluye todos los componentes WAN, LAN, dispositivos de seguridad, y demás dispositivos que soportan al servicio de seguridad, así como su equivalente de configuración lógica.

El origen de medición será por una correlación de los poleos y/o muestras recolectadas cada 5 minutos por el sistema de monitoreo y los períodos de indisponibilidad extraídos de los incidentes abiertos en el sistema de administrador de incidencias del proveedor de SASI 2022-2024, restándosele aquellos períodos de indisponibilidad cuya responsabilidad no sea atribuible al Proveedor de SASI 2022- 2024. La forma de medición en específico se describirá de la siguiente manera.

- Calculada en base a 30 días por mes
- Calculada a partir del inicio de la falla
- Se considera indisponible cuando el protocolo de la interfaz se encuentra caído (Down) o por caída de tráfico imputable a infraestructura del proveedor.
- Solo es calculada en base a fallas imputables al Proveedor de SASI 2022-2024.

**Disponibilidad por sitio y por posición de servicio**
Las caídas originadas por falla de energía responsabilidad del Instituto no serán tomadas en cuenta para la disponibilidad.

$$\text{Disponibilidad\_del\_Servicio} = \left\{ \frac{\text{Tiempo\_Total} - (\text{Tiempo\_Indisponible} - \text{Tiempo\_Instituto})}{\text{Tiempo\_Total}} \right\} X100$$

Dónde:
Tiempo Total: Tiempo total de disponibilidad para el mes de medición.
Tiempo Indisponible: Tiempo indisponible según plataforma de monitoreo.
Tiempo Instituto: Tiempos atribuibles al Instituto extraídos del sistema de administración de incidentes.

**Objetivos por métrica:**

| Disponibilidad Servicio | % Disponibilidad |
|---|---|

| | |
|---|---|
| Servicios de Seguridad – Continuidad Operativa | 99.99% |
| Servicios de Seguridad – Verificación y Calidad | 99.97% |
| Servicios del Centro de Operaciones de Seguridad (SOC) | 99.99% |

**Deductiva por incumplimiento**

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Cuando no se cumplan con los objetivos de servicio, para los diferentes niveles de disponibilidad, conforme al esquema de medición propuesto | % Disponibilidad conforme la tabla de objetivos | Minuto | 0.5% por cada minuto de indisponibilidad | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

### 10.8. Tiempo de detección y solución de fallas

## Partida 1

La métrica de tiempo de solución a fallas es independiente de la métrica de disponibilidad, dado que se refiere al tiempo en el cual será devuelta a la normalidad (restitución de la operación estable) uno o varios servicios al presentarse una falla. Las mediciones de Tiempo de Solución de Fallas deberán ser realizadas por el Proveedor de SASI 2022-2024, usando su correspondiente herramienta de gestión y monitoreo del servicio. El Proveedor deberá realizar esta medición en un periodo mensual considerando el promedio del tiempo de solución para cada tipo de severidad. La metodología que se realice, las herramientas y los responsables sobre las mediciones, quedarán definidos en las mesas de trabajo.

El Tiempo de Solución a Fallas se divide en tres casos, en función de la severidad, causa e impacto de los mismos:

**Severidad Critica**: Representa un incidente de alto impacto dado el riesgo que representa. Este tipo de incidente puede, potencialmente, ocasionar afectación y daño en activos y servicios del cliente. Eventos de afectación total al servicio, pérdida total del sistema de comunicaciones y/o seguridad, degradación de los recursos del Instituto o bien mediante el descubrimiento de vulnerabilidad en la infraestructura protegida. La alarma relativa en el sistema de gestión se mantiene por más de 10 minutos.

**Severidad Alta**: Representa un incidente serio en el que hay una degradación más no una afectación de negocio a los servicios e infraestructura que es protegida mediante los dispositivos de alta disponibilidad o de seguridad. El incidente se manifiesta mediante el bloqueo o bajo desempeño al acceder a ciertos servicios de red que requieren el uso de los dispositivos de comunicaciones y/o seguridad, así como la pérdida parcial de alguna funcionalidad en el equipo de comunicaciones y/o seguridad. Eventos de afectación que ocasionan degradación en el servicio sin llegar a ocasionar caída del mismo.

**Severidad Media**: Representa un incidente menor que no trae consecuencias de impacto de negocio a los servicios e infraestructura protegida por los dispositivos de seguridad. El incidente se da mediante fallas en visualización de bitácoras o problemas para comunicación de servicios internos del Instituto y hacia un grupo reducido de usuarios. Eventos de afectación al servicio por períodos de tiempo menores a 10 minutos ocasionando intermitencia en la disponibilidad del servicio.

**Severidad Baja**: Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad. Estos casos de severidad deben ser atendidos por ingenieros del proveedor de servicios en sitio con la colaboración del fabricante vía un centro de asistencia técnica personalizada. El tiempo de resolución de este tipo de falla será definido por el Instituto y el Proveedor de SASI 2022-2024, al momento de presentar el caso.

La severidad de un incidente es determinada por la convocante. Conforme la operación y criticidad de un servicio, se define la severidad, así como su nivel de escalación, con base en lo siguiente:

| SEVERIDAD | AFECTACIÓN | TIEMPO MÁXIMO DE REGISTRO | TIEMPO MÁXIMO DE SOLUCIÓN |
|---|---|---|---|
| **Critica** | Representa una falla de alto impacto que impide la operación total de un servicio, mismo que soporta una función de negocio del Instituto a nivel nacional. | 10 minutos posteriores a la detección de la falla | 2 horas posteriores al registro y notificación de la falla |
| **Alta** | Representa una falla en la que hay una degradación que impide la operación de un servicio, mismo que soporta una función de negocio del Instituto pero que no tiene un impacto a nivel nacional. | 20 minutos posterior a la detección de la falla | 4 horas posterior al registro y notificación de la falla |

| | | | |
|---|---|---|---|
| **Media** | Representa una falla menor que impide la operación de un servicio, mismo que afecta a un grupo de usuarios reducido del Instituto. | 120 minutos posterior a la detección de la falla | 48 horas posterior al registro y notificación de la falla |
| **Baja** | Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad, tienen un bajo impacto en la operación del negocio y su atención y/o solución puede ser calendarizada. | 5 días hábiles posterior a la detección de la falla | Se define entre el Instituto y el Proveedor de SASI 2022-2024 conforme las mesas de trabajo que se establezcan para este propósito. |

**Deductivas por incumplimiento**

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Tiempo máximo de registro y notificación conforme al nivel de severidad critica | 10 minutos posteriores al registro y notificación de la falla | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad critica | 2 horas posteriores al registro y notificación de la falla | Hora | 0.5% por cada hora o fracción de atraso en la solución de la falla | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel | 20 minutos posteriores al registro y | Minuto | 0.2% por cada minuto de atraso en el | Valor unitario de la facturación mensual del servicio |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| de severidad alta | notificación de la falla | | registro y notificación | relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad alta | 4 horas posteriores a la registro y notificación de la falla | Hora | 0.5% por cada hora o fracción de atraso en la solución de la falla | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de severidad media | 120 minutos posteriores al registro y notificación de la falla | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad media | 48 horas posteriores al registro y notificación de la falla | Hora | 0.5% por cada hora o fracción de atraso en la solución de la falla | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de severidad baja | 5 días hábiles posteriores al registro y notificación de la falla | Día | 0.2% por cada día hábil de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad baja | Se define entre el Instituto y el Proveedor de SASI 2022-2024 conforme las mesas de trabajo que se | Día | 0.5% por cada día de atraso en la solución de la falla conforme la fecha establecida en las mesas de trabajo | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| | establezcan para este propósito. | | | |

### 10.9. Tiempo de detección y mitigación de incidentes

**Partida 1**

Una actividad sospechosa son acciones que pudieran estar encaminadas a comprometer la seguridad de la red y de los activos de información, es la etapa previa a la materialización de un incidente de seguridad. Un incidente de seguridad es el registro de una violación a las políticas de seguridad informática o al uso aceptable de políticas o de prácticas de seguridad estandarizado; es la evidencia inequívoca de que la confidencialidad, integridad y disponibilidad de la información ha sido vulnerada.

Las métricas de tiempo para la actividad sospechosa se refieren al tiempo de notificación y envió de dictamen que el proveedor SASI 2022-2024 deberá realizar ante el Instituto al momento de detectar una actividad sospechosa. Ante una actividad sospechosa, el proveedor del SASI 2022-2024 deberá registrar y notificar al personal del Instituto en máximo 30 minutos. Posterior a su detección y registro, se deberá emitir un dictamen de actividad sospechosa con recomendaciones para erradicarla, este dictamen será enviado al personal del Instituto en máximo 90 minutos.

Las métricas para el tiempo de registro y notificación se refieren al tiempo en que proveedor SASI 2022-2024 avisa al Instituto cuando ha confirmado un incidente de seguridad, ésta métrica deberá realizarse en los tiempos definidos según la prioridad a partir de que se apertura algún registro relacionado con un incidente de seguridad. La métrica de tiempo de contención se refiere a que, tras la detección del incidente, el Proveedor de SASI 2022-2024 deberá detener y aislar el mismo según los tiempos definidos para cada prioridad.

Las mediciones deberán ser realizadas por el proveedor de SASI 2022-2024, usando su correspondiente herramienta de gestión y monitoreo del servicio. El proveedor deberá realizar esta medición en un periodo mensual según el nivel de servicio para cada tipo de métrica y/o prioridad.

**Objetivos de la métrica**

| SEVERIDAD | AFECTACIÓN | TIEMPO MÁXIMO DE REGISTRO | TIEMPO MÁXIMO DE SOLUCIÓN |
|---|---|---|---|
| **Critica** | Representa un incidente de alto impacto que impide la operación total de | 10 minutos posteriores a la detección del incidente | 60 minutos posteriores al registro y |

| SEVERIDAD | AFECTACIÓN | TIEMPO MÁXIMO DE REGISTRO | TIEMPO MÁXIMO DE SOLUCIÓN |
|---|---|---|---|
| | un servicio, mismo que soporta una función de negocio del Instituto a nivel nacional. | | notificación del incidente |
| **Alta** | Representa un incidente en el que hay una degradación que impide la operación de un servicio, mismo que soporta una función de negocio del Instituto pero que no tiene un impacto a nivel nacional. | 20 minutos posterior a la detección del incidente | 240 minutos posteriores al registro y notificación del incidente |
| **Media** | Representa un incidente menor que impide la operación de un servicio, mismo que afecta a un grupo de usuarios reducido del Instituto. | 30 minutos posterior a la detección del incidente | 60 minutos posteriores al registro y notificación del incidente |
| **Baja** | Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad, tienen un bajo impacto en la operación del negocio y su atención y/o solución puede ser calendarizada. | 60 minutos posterior a la detección del incidente | 2,880 minutos posteriores al registro y notificación del incidente |

**Deductiva por incumplimiento**

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Registro y notificación de Actividad Sospechosa | 30 minutos posteriores a la detección actividad sospechosa | Minuto | 0.5% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Envío de Dictamen de Actividad Sospechosa | 90 minutos posteriores al registro y notificación de actividad sospechosa | Minuto | 1% por cada minuto de atraso en la elaboración del dictamen | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Tiempo máximo de registro y notificación conforme al nivel de severidad critica | 10 minutos posteriores al registro y notificación del incidente | Minuto | 0.5% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad critica | 60 minutos posteriores al registro y notificación del incidente | Minuto | 1% por cada minuto de atraso en la solución del incidente | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación | 20 minutos posteriores al registro y | Minuto | 0.5% por cada minuto de atraso en el | Valor unitario de la facturación mensual del |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| conforme al nivel de severidad alta | notificación del incidente | | registro y notificación | servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad alta | 240 minutos posteriores al registro y notificación del incidente | Minuto | 1% por cada minuto de atraso en la solución del incidente | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de severidad media | 30 minutos posteriores al registro y notificación del incidente | Minuto | 0.5% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad media | 1,440 minutos posteriores al registro y notificación del incidente | Minuto | 1% por cada minuto de atraso en la solución del incidente | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de severidad baja | 60 minutos posteriores al registro y notificación del incidente | Minuto | 0.5% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad baja | 2,880 minutos posteriores al registro y notificación del incidente | Minuto | 1% por cada minuto de atraso en la solución del incidente | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

**10.10. Solicitudes de requerimientos y cambios**

## Partida 1

Es el tiempo que tarda el Proveedor de SASI 2022-2024, en realizar una alta, cambio o baja sobre la infraestructura del servicio en seguridad, basada en el menú de configuraciones comunes preestablecidas durante las mesas de trabajo correspondientes. Estas configuraciones deberán ser acorde a las necesidades de conectividad y flujos de información de las aplicaciones del Instituto, entendiendo que la complicación para su atención es menor dado que se tiene la experiencia y el conocimiento de las mismas configuraciones de los módulos de los servicios de seguridad en operación.

**Objetivos de la métrica:**

| PRIORIDAD | DESCRIPCIÓN | TIEMPO MÁXIMO DE REGISTRO | TIEMPO MÁXIMO DE EJECUCIÓN |
|---|---|---|---|
| **Alta** | Requerimiento generado por parte del Instituto a fin de atender a necesidades de operación emergentes. | 10 minutos posteriores a la solicitud formal por parte del Instituto | 60 minutos posteriores al registro realizado por el Instituto |
| **Media** | Requerimiento generado por parte del Instituto a fin de atender a necesidades de operación comunes. | 30 minutos posteriores a la solicitud formal por parte del Instituto | 480 minutos posteriores al registro realizado por el Instituto |
| **Baja** | Requerimiento generado por parte del Instituto a fin de atender a necesidades de operación programadas. | 60 minutos posteriores a la solicitud formal por parte del Instituto | 1,440 minutos posteriores al registro realizado por el Instituto |

**Cambios**

| PRIORIDAD | DESCRIPCIÓN | TIEMPO MÁXIMO DE REGISTRO | TIEMPO MÁXIMO DE EJECUCIÓN |
|---|---|---|---|
| **Emergente** | Cambios requeridos como resultado de una | 1 hora posteriores a | Conforme al plan de trabajo definido |



DIVISIÓN DE CONTRATOS

| PRIORIDAD | DESCRIPCIÓN | TIEMPO MÁXIMO DE REGISTRO | TIEMPO MÁXIMO DE EJECUCIÓN |
|---|---|---|---|
| | pérdida repentina del servicio, falla en un activo de infraestructura o a petición del Instituto. | la solicitud formal por parte del Instituto | entre el Instituto y el Proveedor |
| **Normal** | Cambios solicitados para mejorar o restaurar un servicio o ampliar un activo de infraestructura, que no están considerados en el catálogo de cambios estándar, mismos que deben ser analizados y aprobados por el Instituto. | 1 hora posteriores a la solicitud formal por parte del Instituto | Conforme al plan de trabajo definido entre el Instituto y el Proveedor |
| **Estándar** | Cambios en los servicios y/o activos de infraestructura que se realiza en línea y sigue una trayectoria establecida, mismos que representan una solución aceptada a un requerimiento o conjunto de requerimientos específicos. | 1 hora posteriores a la solicitud formal por parte del Instituto | 24 horas posterior al registro realizado por el Instituto |

Cualquier cambio ejecutado por el Proveedor, mismo que no se encuentre autorizado por el Instituto, derive o no en alguna falla de los servicios de seguridad, será catalogado como un incidente de seguridad, mismo que será clasificado con base en las afectaciones o riesgos que pudieron generar.

**Deductiva por incumplimiento:**

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Tiempo máximo de registro y notificación conforme al nivel de prioridad Alta | 10 minutos posteriores al registro y notificación del requerimiento | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de ejecución conforme al nivel de prioridad Alta | 60 minutos posteriores al registro y notificación del requerimiento | Minuto | 0.5% por cada minuto de atraso en la ejecución del requerimiento | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de prioridad Media | 30 minutos posteriores al registro y notificación del requerimiento | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de prioridad Media | 8 horas posteriores al registro y notificación del requerimiento | Hora | 0.5% por cada hora o fracción de atraso en la ejecución del requerimiento | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de prioridad Baja | 60 minutos posteriores al registro y notificación del requerimiento | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Tiempo máximo de solución conforme al nivel de prioridad Baja | 24 horas posteriores al registro y notificación del requerimiento | Hora | 0.5% por cada hora o fracción de atraso en la ejecución del requerimiento | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

**Cambios**

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Tiempo máximo de registro y notificación conforme al nivel de prioridad Emergente | 60 minutos posteriores al registro y notificación del cambio | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de ejecución conforme al nivel de prioridad Emergente | Conforme al plan de trabajo definido entre el Instituto y el Proveedor | Hora | 1% por cada hora o fracción de atraso en la ejecución del cambio | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de prioridad Normal | 60 minutos posteriores al registro y notificación del cambio | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel | Conforme al plan de trabajo definido entre | Hora | 1% por cada hora o fracción de atraso en la | Valor unitario de la facturación mensual del servicio |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| de prioridad Normal | el Instituto y el Proveedor | | ejecución del cambio | relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de prioridad Estándar | 60 minutos posteriores al registro y notificación del cambio | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de prioridad Estándar | 24 horas posteriores al registro y notificación del cambio | Hora | 1% por cada hora o fracción de atraso en la ejecución del cambio | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

**10.11. Servicios de Seguridad – Continuidad Operativa**

**Partida 1**

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Reportes Técnicos de los activos de infraestructura que contemplen:<br>• Disponibilidad<br>• Controles de Cambios<br>• Requerimientos<br>• Incidentes/Fallas<br>• Actividad Sospechosa<br>• Estadísticas de uso de los | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| servicios (conforme la definición en las mesas de trabajo) | | | | |

**10.12. Servicios de Seguridad – Verificación/Calidad**

**Partida 1**

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Reportes Técnicos de los activos de infraestructura que contemplen:<br>• Disponibilidad<br>• Controles de Cambios<br>• Requerimientos<br>• Incidentes/Falla<br>• Actividad Sospechosa<br>• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Servicios de Borrado Seguro de Información: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado. | 5 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Servicio de Gestión de Dominios: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de | 5 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |



DIVISIÓN DE CONTRATOS

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| los dominios que se hayan renovados adquiridos. | | | | |
| Servicio de Certificados Digitales SSL: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los certificados que se hayan renovado o adquiridos (incluyendo archivo electrónico compreso con la llave publica relacionado con los requerimientos) | 1 día hábil posterior a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Servicios de Ciberinteligencia: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de amenazas y ataques potenciales a los que se encuentra expuesto el Instituto que incluya: Situación general del evento, | 1 día hábil posterior a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| hallazgos detectados, mecanismos de inteligencia accionable, táctica u operativa recomendados para prevención y/o contención | | | | |
| Servicios de Sistema de Gestión de Seguridad de la Información: Plan de Trabajo de implementación y operación de los servicios conforme al alcance definido en las mesas de trabajo | 10 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del plan de trabajo | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Servicios de Sistema de Gestión de Seguridad de la Información: Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora del Sistemas De Gestión de | Conforme a la fecha estipulada en el plan de trabajo acordado entre el Instituto y el Proveedor | Día | 1% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, por evento | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Seguridad de la Información (SGSI) | | | | |
| Servicios de Gestión del Cambio en Seguridad de la Información: Plan de Trabajo de implementación y operación de los servicios conforme al alcance definido en las mesas de trabajo | 10 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del plan de trabajo | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Servicios de Gestión del Cambio en Seguridad de la Información: Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora de la Gestión del Cambio en Seguridad de la Información | Conforme a la fecha estipulada en el plan de trabajo acordado entre el Instituto y el Proveedor | Día | 1% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, por evento | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

**Partida 2**

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Servicio de Análisis de Vulnerabilidades Estático<br>Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada pieza de software (código) escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el | 7 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| proceso de análisis | | | | |
| Servicio de Análisis de Vulnerabilidades Dinámico<br>Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las | 7 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| herramientas tecnológicas utilizadas para el proceso de análisis | | | | |
| Servicios de Pruebas de Penetración:<br><br>Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los | 10 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis | | | | |
| Servicios de Análisis Forense: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de infraestructura verificados | 15 días hábiles posterior a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

**10.13. Servicios del Centro de Operaciones de Seguridad (SOC)**

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos | Valor unitario de la facturación mensual del servicio relacionado con |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| los servicios de seguridad implementados | | | | el incumplimiento |
| Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes de estadísticas | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| definiciones realizadas en las mesas de trabajo | | | | |
| Reporte de las evaluaciones operativas a los servicios de seguridad implementados | 5 días hábiles posteriores al cumplimiento de cada trimestre vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes de estadísticas | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte que integre el calendario de actualizaciones de versionamiento en software de cada servicio implementados | 5 días hábiles posteriores al cumplimiento de cada trimestre vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes de estadísticas | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Creación de cuentas de acceso en las consolas de administración de los servicios de seguridad | 5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto | Día | 1% por cada día hábil de atraso en la entrega de las cuentas de acceso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Creación de cuentas de acceso en la base de conocimientos de | 5 días hábiles posteriores al término de la implementación de cualquier solución de | Día | 1% por cada día hábil de atraso en la entrega de las cuentas de acceso | Valor unitario de la facturación mensual del servicio relacionado con |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| las soluciones de seguridad | seguridad o conforme a cada solicitud generada por el Instituto | | | el incumplimiento |
| Actualización de la matriz de escalación | 5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad | Día | 1% por cada día hábil de atraso en la entrega de la matriz de escalación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad | 5 días hábiles posteriores a la ejecución de la ventana mantenimiento | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad | 5 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del reporte | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte Técnico de las configuraciones de las soluciones de seguridad | 5 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del reporte técnico | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Reporte Técnico de los incidentes presentados en las soluciones de seguridad | 5 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del reporte técnico | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte Técnico de los requerimientos registrados en la mesa de servicios | 5 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del reporte técnico | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y su diagrama de interrelación conforme fueron registrados en la CMDB | 5 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del reporte técnico | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Diagramas de Arquitectura de las soluciones de seguridad | 2 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del reporte técnico | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tablero de Estadísticas de Servicios de | 10 días hábiles posteriores al término de la | Día | 1% por cada día hábil de atraso en la | Valor unitario de la facturación mensual del |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Seguridad (Portal Único) | habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo | | entrega de los reportes de actividades, por periodo, por evento | servicio relacionado con el incumplimiento |

Cualquier cambio ejecutado por el SOC, mismo que no se encuentre autorizado por el Instituto, derive o no en alguna falla de los servicios de seguridad, será catalogado como un incidente de seguridad, mismo que será clasificado con base en las afectaciones o riesgos que pudieron generar.

## 11. Condiciones de Pago

Como se establece en el presente documento, el administrador de contrato será el servidor público responsable de supervisar que se cumplan en tiempo y forma los compromisos contenidos en el contrato que para tal efecto se celebre.

Los pagos se realizarán previa validación y aceptación de los servicios por parte del Administrador del Contrato, es decir, el Titular de la División de Seguridad Informática Física, que reciba cada uno de los servicios y que será responsable de realizar los trámites de pago en estricto apego al procedimiento administrativo vigente en el instituto.

Para proceder a la liberación de pago, el Titular de la División de Seguridad Informática Física o el Servidor Público que para tal efecto haya designado el Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información, será responsable de la supervisión y administración de todas las obligaciones a cargo del proveedor.

Así como de la ejecución, validación, técnica y administrativamente de todos y cada uno de los documentos que acreditan que los servicios proporcionados por el proveedor se cumplieron en tiempo, forma y cantidad con las características, especificaciones y condiciones contractualmente pactadas para el proyecto, procederá de conformidad con lo establecido en el artículo 51 de la LAASSP, la forma de pago al proveedor será la estipulada en los contratos y quedará sujeta a las condiciones que establezcan las mismas; sin

embargo, no podrá exceder de veinte días naturales contados a partir de la entrega de la factura respectiva, previa entrega de certificado de licencia o de la prestación de los servicios en los términos del contrato.

El proveedor deberá entregar en la División de Trámite de Erogaciones, situada en la calle de Gobernador Tiburcio Montiel No. 15, PB, Col. San Miguel Chapultepec, Código Postal 11850, Delegación Miguel Hidalgo, México, D.F., en días y horas hábiles, los siguientes documentos:

- Original y copia de la factura que expida el Proveedor, a nombre del Instituto Mexicano del Seguro Social, con dirección en Av. Paseo de la Reforma N° 476, Col. Juárez, Delegación Cuauhtémoc, C.P. 06600, México, D.F., y R.F.C. IMS-421231-I45; que reúna los requisitos fiscales, en la que se indiquen los servicios proporcionados y el número de contrato que ampara dichos servicios,
- Original y Copia de la documentación que avale la entrega de los servicios a satisfacción de el instituto (Acta Entrega-Recepción de los Servicios).
- Carta firmada por el representante legal, en la cual haga del conocimiento de el instituto la cuenta bancaria a la que se efectuará la transferencia electrónica bancaria correspondiente.
- Nota de crédito (en caso de que aplique) a favor del Instituto Mexicano del Seguro Social por el importe de la sanción en caso de entrega extemporánea de los servicios contratados.
- Presentará Orden de Ingreso (Nota de Crédito) (en caso de que aplique para Soporte Técnico dentro de los primeros 10 días hábiles después de la fecha del Acta Entrega-Recepción de los Servicios del trimestre firmada, a favor del Instituto Mexicano del Seguro Social por el importe de la sanción en caso de entrega extemporánea de los servicios contratados, en caso de no entregar la Orden de ingreso (Nota de Crédito) correspondiente al plazo citado en este punto, se aplicara la ejecución de garantía.

En caso de que el proveedor presente sus facturas con errores o deficiencias, estos se le harán saber por parte de el instituto dentro del término estipulado para ello, y el plazo de pago se ajustará, debiendo presentar nuevamente toda la documentación mencionada anteriormente (en original y/o copia, según corresponda).

El Pago se realizará en pesos mexicanos, en pagos pagos progresivos a mes vencido conforme a las entregas programadas.

## 12. Entregables

El proveedor deberá entregar al Titular de la División de Seguridad Informática Física dependiente de la Coordinación de Telecomunicaciones y Seguridad de la Información los siguientes:

### 12.1. Entregables Generales

**Partida 1**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Habilitación, Operación y Transición | Plan de Trabajo Detallado de los servicios del proyecto | Única Vez | 15 días naturales posteriores a la emisión del fallo |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | Documento Compromiso de suscripción del acuerdo de niveles operacional (*Operational Level Agreement,* OLA) | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Matriz de Escalación | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| Servicios de Seguridad – Continuidad Operativa | Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto | Única Vez | 5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas | Única Vez | 10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | | | integrada y posterior a la integración de las mesas de trabajo |
| | Memorias Técnicas Actualizadas de las Servicios de Seguridad | Única Vez | 20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados |
| Servicios de Seguridad – Verificación/Calidad | Documento con el diseño de Alto Nivel de los servicios de Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integran activos de infraestructura para su habilitación | Única Vez | 5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integran activos de infraestructura para su habilitación | Única Vez | 10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo |
| | Memorias Técnicas Actualizadas de las Servicios de Seguridad, que | Única Vez | 20 días hábiles previo al término del contrato para aquellos |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | requieran integran activos de infraestructura para su habilitación | | servicios que se encuentren habilitados |
| Servicios de Borrado Seguro de Información | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicio de Gestión de Dominios | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicio de Certificados Digitales SSL | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Sistema de Gestión de Seguridad de la Información (SGSI) | Metodología para la continuidad de los servicios | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Gestión del Cambio en Seguridad de la Información | Metodología para la implementación de los servicios | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Procesos de operación implementados:<br>• Requerimientos<br>• Cambios<br>• Configuraciones<br>• Incidentes<br>• Problemas<br>• Monitoreo | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Matriz de Escalación Técnica y Organizacional | Única Vez | 15 días naturales posteriores a la emisión del fallo |



ANEXOS
DIVISIÓN DE CONTRATOS

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | Procedimiento de operación de la Mesa de Servicios:<br>• Requerimientos<br>• Cambios<br>• Configuraciones<br>• Incidentes<br>• Problemas<br>• Monitoreo | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Expedientes Curriculares del personal del SOC | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| Tablero de Estadísticas de Servicios de Seguridad (Portal Único) | Creación de cuentas de acceso en portal único de las soluciones de seguridad | Única Vez | 10 días hábiles posteriores al término de la habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo |

**Partida 2.**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Habilitación, Operación y Transición | Plan de Trabajo Detallado de los servicios del proyecto | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Documento Compromiso de suscripción del acuerdo de niveles operacional (*Operational Level Agreement*, OLA) | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Matriz de Escalación | Única Vez | |

| | | | |
|---|---|---|---|
| | | | 15 días naturales posteriores a la emisión del fallo |
| | Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| Servicios de Análisis de Vulnerabilidades Dinámico | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Pruebas de Penetración | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Análisis Forense | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Análisis de Vulnerabilidades Estático | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |

### 12.2. Entregables bajo demanda

El proveedor, de manera enunciativa más no limitativa, deberá generar entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

**Partida 1**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Borrado Seguro de Información | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado. | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicio de Gestión de Dominios | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos. | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicio de Certificados Digitales SSL | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los certificados que se hayan renovado o adquiridos (incluyendo archivo electrónico compreso con la llave publica relacionado con los requerimientos) | Evento | 1 día hábil posteriores a la solicitud generada por parte del Instituto |
| Servicios de Sistema de Gestión de Seguridad de la Información | Plan de Trabajo de continuidad y operación de los servicios conforme al | Evento | 10 días hábiles posteriores a la solicitud generada por parte del Instituto |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | alcance definido en las mesas de trabajo | | |
| Servicios de Gestión del Cambio en Seguridad de la Información | Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo | Evento | 10 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad | Evento | 5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto |
| | Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad | Evento | 5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme cada solicitud generada por el Instituto |
| | Actualización de la matriz de escalación | Evento | 5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad y Red |
| | Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad y red | Evento | 5 días hábiles posteriores a la ejecución de la ventana mantenimiento |
| | Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad y red | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Reporte Técnico de las configuraciones de | Evento | 5 días hábiles posterior a la solicitud |



ANEXOS
DIVISIÓN DE CONTRATOS

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | las soluciones de seguridad y red | | generada por parte del Instituto |
| | Reporte Técnico de los incidentes presentados en las soluciones de seguridad y red | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Reporte Técnico de los requerimientos registrados en la mesa de servicios | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y red, así como su diagrama de interrelación conforme fueron registrados en la CMDB | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Diagramas de Arquitectura de las soluciones de seguridad y red | Evento | 2 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | | | |

**Partida 2**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Análisis de Vulnerabilidades Dinámico | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada | Evento | 7 días hábiles posteriores a la solicitud generada por parte del Instituto |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis | | |
| Servicios de Prueba de Penetración | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya | Evento | 10 días hábiles posteriores a la solicitud generada por parte del Instituto |



ANEXOS
DIVISIÓN DE CONTRATOS

2022 Año de Ricardo Flores Magón

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis | | |
| Servicios de Análisis Forense | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de infraestructura verificados | Evento | 15 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicios de Análisis de Vulnerabilidades Estático | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada pieza de software (codigo) analizados indicando al menos: aplicativo relacionado, fecha de análisis, código fuente analizado, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis | Evento | 10 días hábiles posteriores a la solicitud generada por parte del Instituto |

**12.3. Entregables Periódicos**

El proveedor, de manera enunciativa más no limitativa, deberá generar entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

**Partida 1**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Seguridad – Continuidad Operativa | Reportes Técnicos de los activos de infraestructura que contemplen:<br>• Disponibilidad<br>• Controles de Cambios<br>• Requerimientos<br>• Incidentes/Fallas<br>• Actividad Sospechosa<br>• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| Servicios de Seguridad – Verificación/Calidad | Reportes Técnicos de los activos de infraestructura que contemplen:<br>• Disponibilidad<br>• Controles de Cambios<br>• Requerimientos<br>• Incidentes/Fallas<br>• Actividad Sospechosa<br>• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte de las evaluaciones operativas a los servicios de seguridad implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |
| | Reporte que integre el calendario de actualizaciones de versionamiento en *software* de cada servicio implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |

**Partida 2**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Análisis de Vulnerabilidades Dinámico | Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| Servicios de Análisis de Vulnerabilidades Estático | Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| Servicios de Pruebas de Penetración | Reporte de las evaluaciones operativas a los servicios de seguridad implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Análisis Forense | Reporte que integre el calendario de actualizaciones de versionamiento en *software* de cada servicio implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |

Los entregables requeridos durante la vigencia del contrato, deberán ser entregados en formato electrónico (MS Word, MS Excel, PDF) conforme los periodos estipulados por el Instituto.

De igual manera, el proveedor deberá establecer un repositorio digital, que, de manera alterna, servirá para alojar los entregables antes señalados, mismos que estarán disponibles para su consulta durante la vigencia del contrato, teniendo en cuenta que el Instituto definirá en las mesas de trabajo los permisos de acceso correspondientes para el administrador del contrato, cuerpo de gobierno que se conforme para este propósito u otros funcionaros que sean designados por el primero mencionado.

## 13. Condiciones de aceptación de los servicios

1. Se deberán formalizar los entregables descritos en el numeral anterior a efecto de dar por recibido los servicios requeridos.

2. Todos los documentos deben ser entregados en papel membretado de la empresa de manera impresa y en electrónico.

3. Se entregará a la División de Seguridad Informática Física perteneciente a la Coordinación de Telecomunicaciones y Seguridad de la Información.

## 14. Lugar y horario para la entrega

- La entrega se realizará en las instalaciones de el Instituto ubicadas en la calle de Avenida Paseo de la Reforma 476, Anexo de Telecomunicaciones Planta Alta, Colonia Juárez, Delegación Cuauhtémoc, Ciudad de México, C.P. 06600.
- El horario para la entrega será de las 9:00 horas a las 17:00 horas
- En caso de contingencia podrá solicitarse la entrega de las cartas requeridas en el presente documento en cualquiera de los inmuebles que formen parte de las Oficinas Centrales de el instituto, ubicadas en la Colonia Juárez, Delegación Cuauhtémoc, C.P. 06600 en la Ciudad de México.

## 15. Convenio de Confidencialidad y Resguardo de la Información

El "Licitante" deberá suscribir el Convenio de Confidencialidad y Resguardo de Información Correspondiente con la persona designada como Administradora de Contrato. En complemento, el "Licitante" deberá considerar al menos los siguientes mecanismos de control de acceso a la información del IMSS:

a. Se deberán establecer controles de acceso y privilegios restringidos al personal del "Licitante", a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del IMSS.

b. El "Licitante" deberá implantar y aceptar en todo momento el uso de controles que permitan "Pistas de Auditoria" para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.

c. La seguridad lógica deberá estar protegida mediante el uso de "Firewalls", mecanismos de encriptación y seguridad física entre las redes del "Licitante" y las del IMSS.

d. El "Licitante" deberá contar con sistemas que contengan una administración estricta de registros y políticas de retención de la información del IMSS.

e. Los empleados del "Licitante" con acceso a la información sensible del IMSS, deberán firmar acuerdos de confidencialidad con este.

f. El almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por el "Licitante" de los servicios de SASI 2022- 2024 observando los requisitos de seguridad y resguardo de la información.

g. El uso de *hardware* que podría ser utilizado para copiar datos y extraer información, como son dispositivos removibles, quemado de CD y dispositivos de memoria "Flash-USB", entre otros, por parte del personal del "Licitante" serán restringidos y deberán observar las políticas de seguridad del IMSS al respecto.

h. El "Licitante" deberá permitir el acceso a información relacionada con el servicio prestado al IMSS para la realización de auditorías.

i. El "Licitante" no deberá hacer uso indebido de la documentación, información, ni activos de TIC a los que tengan acceso o que se generen con motivo de la prestación del servicio.

## 16. Propiedad Intelectual

El proveedor se obliga durante la garantía de las licencias a liberar a el Instituto de toda responsabilidad de carácter civil, mercantil, penal o administrativa que, en su caso, se ocasione con motivo de la infracción de derechos de autor, patentes, marcas u otros derechos de propiedad industrial o intelectual a nivel Nacional o Internacional.

## 17. Método de evaluación de propuestas

Se evaluará mediante el procedimiento de puntos y porcentajes, conforme a las características que presenten los proveedores en cuanto a funcionalidades requeridas en el Anexo Técnico, de acuerdo con la poderación establecida en la matriz de evaluación correspondiente.

## 18. Funcionarios públicos de la DIDT participantes en el proceso de contratación

a) C. Florencio Fernando González Velázquez, Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información.
b) C. Abraham Gutiérrez Castillo, Titular de la División de Seguridad Informática Física.
c) C. Cynthia Osmara Verdin Villegas, Jefe Área Nivel Central.

**19. Vigencia del Contrato**

La vigencia del contrato será a partir del día hábil siguiente a la notificación del fallo y hasta el 30 de septiembre de 2024.

**20. Plazo del servicio**

La prestación de los servicios iniciará a partir del día hábil siguiente a la notificación del fallo y hasta el 30 de septiembre de 2024.

**21. Administrador del Contrato**

Conforme a las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto, el Administrador del Contrato, será el responsable de supervisar que se cumplan en tiempo y forma los compromisos contenidos en el contrato que para tal efecto se celebre, por lo que:

a) **Administrador del Contrato y Responsable Técnico**; Titular de la División de Seguridad Informática Física.

b) **Supervisor del Contrato**; Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información.

Los servicios a cargo del proveedor estarán bajo la administración y supervisión del responsable designado que para tal efecto.

**22. Mecanismos de control para la administración del contrato**

El Administrador del Contrato en conjunto con el proveedor deberá generar el acta de entrega-recepción conforme a lo establecido en el Anexo Técnico.

**23. Mecanismos requeridos al proveedor para responder por defectos o vicios ocultos de los bienes o de la calidad de los servicios**

No aplica



ANEXO 3
DIVISIÓN DE CONTRATOS

## 24. Otorgamiento de anticipo

No aplica

| | | |
|---|---|---|
| IMSS | INSTITUTO MEXICANO DEL SEGURO SOCIAL<br>DIRECCIÓN DE ADMINISTRACIÓN<br>UNIDAD DE ADQUISICIONES<br>COORDINACIÓN DE ADQUISICIÓN DE BIENES Y<br>CONTRATACIÓN DE SERVICIOS<br>COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS | CONTRATO<br>NÚMERO<br>019E18222-001 |

# ANEXO 3 (TRES)

## "PROPUESTA TÉCNICA Y ECONÓMICA DE "EL PROVEEDOR" Y ACTA DE FALLO"

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

# INSTITUTO MEXICANO DEL SEGURO SOCIAL

## DIRECCIÓN DE ADMINISTRACIÓN
## UNIDAD DE ADQUISICIONES
## COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS
## COORDINACIÓN TÉCNICA DE ADQUISICIÓN DE BIENES DE INVERSIÓN Y ACTIVOS
## DIVISIÓN DE CONTRATACIÓN DE ACTIVOS Y LOGÍSTICA.

## CONVOCATORIA
## LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
## NÚM. LA-050GYR019-E182-2022

## PARA LA CONTRATACIÓN DE LOS:
## "SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024"

## PROPUESTA TÉCNICA.

ANEXOS
DIVISIÓN DE CONTRATOS

Índice de la Propuesta.

ÍNDICE DE LA PROPUESTA ..... 2
PROPUESTA TÉCNICA ..... 6
1. OBJETIVO DEL DOCUMENTO ..... 6
1.1. OBJETIVO GENERAL ..... 6
1.2. OBJETIVOS ESPECÍFICOS ..... 6
OPERBES S.A. DE C.V. TOMÓ EN CONSIDERACIÓN LO SIGUIENTE ..... 6
2. ALCANCE ..... 7
3. BENEFICIOS ..... 7
4. ACTUALIZACIÓN TECNOLÓGICA ..... 8
5. REQUERIMIENTOS DEL SERVICIO ..... 10
6. REQUERIMIENTOS DEL SERVICIO - ESPECIFICACIONES TÉCNICAS ..... 11
6.1. SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA ..... 11
6.1.1. SERVICIOS DE FIREWALL ..... 11
6.1.2. SERVICIOS DE PREVENCIÓN DE INTRUSOS (IPS) ..... 13
6.1.3. SERVICIOS DE PROTECCIÓN CONTRA ATAQUES DENEGACIÓN DE SERVICIO (DDOS) ..... 16
6.1.4. SERVICIOS DE REDES PRIVADAS VIRTUALES (VPN) ..... 18
6.1.5. SERVICIOS DE FILTRADO DE CONTENIDO WEB ..... 21
6.1.6. SERVICIOS DE FILTRADO DE CONTENIDO DE CORREO (ANTISPAM) ..... 23
6.1.7. SERVICIOS DE FIREWALL ESPECIALIZADO EN SERVICIOS WEB (WAF) ..... 26
6.1.8. SERVICIOS DE FIREWALL ESPECIALIZADO EN BASE DE DATOS (DBF) ..... 29
6.1.9. SERVICIOS DE GESTIÓN UNIFICADA DE AMENAZAS (UTM) ..... 32
6.1.10. SERVICIO DE CORRELACIÓN DE EVENTOS ..... 34
6.1.11. SERVICIO DE PROTECCIÓN DE AMENAZAS PERSISTENTES AVANZADAS (APT) ..... 36
6.2. SERVICIOS DE SEGURIDAD – VERIFICACIÓN Y CALIDAD ..... 38
6.2.1. SERVICIOS DE BORRADO SEGURO DE INFORMACIÓN ..... 39
6.2.2. SERVICIO DE GESTIÓN DE DOMINIOS ..... 41

6.2.3. SERVICIO DE CERTIFICADOS DIGITALES SSL ..... 41
6.2.4. SERVICIOS DE CIBERINTELIGENCIA (CIBERSEGURIDAD) ..... 42
6.2.5. SERVICIOS DE PROTECCIÓN EN REDES INALÁMBRICAS Y SEGURIDAD EN DISPOSITIVOS MÓVILES. ..... 44
6.2.6. SERVICIOS DE GESTIÓN Y CONTROL DE ACCESO PARA USUARIOS PRIVILEGIADOS (AAA) ..... 46
6.2.7. SERVICIO DE ANTIVIRUS ..... 48
6.2.8. SERVICIOS DE PREVENCIÓN DE PÉRDIDA DE INFORMACIÓN ..... 50
6.2.9. SERVICIOS DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) ..... 51
6.2.10. SERVICIOS CONTINUIDAD DE GESTIÓN DEL CAMBIO EN SEGURIDAD DE LA INFORMACIÓN ..... 54
6.3. SERVICIOS DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC) ..... 56
6.5. CONDICIONES PARA LA IMPLEMENTACIÓN DE LOS SERVICIOS ..... 61
6.6. IMPLEMENTACIÓN DE LOS SERVICIOS ..... 62
6.7. MESAS DE TRABAJO ..... 62
6.8. PERFIL DEL PROVEEDOR ..... 64
7. CONDICIONES TÉCNICAS DE ACEPTACIÓN DE ENTREGABLES ..... 68
7.1. ENTREGABLES GENERALES ..... 68
7.2. ENTREGABLES BAJO DEMANDA ..... 72
7.3. ENTREGABLES PERIÓDICOS ..... 75
8. NIVELES DE SERVICIO QUE DEBERÁN CUMPLIRSE (SLA) ..... 76
8.1. PENAS CONVENCIONALES ..... 77
9. DEDUCCIONES ..... 77
10. CONVENIO DE CONFIDENCIALIDAD Y RESGUARDO DE LA INFORMACIÓN ..... 77
11. NORMAS ..... 78
12. NORMATIVIDAD APLICABLE ..... 78
13. CUMPLIMIENTO DE POLÍTICAS ..... 78
14. FINALIZACIÓN DEL CONTRATO ..... 79
15. MODELO DE GOBIERNO ..... 79

ANEXOS
DIVISIÓN DE CONTRATOS

APÉNDICE "A" ..... 81
APÉNDICE "B" ..... 114
APÉNDICE "B-BIS" ..... 117
ANEXO 2.- TÉRMINOS Y CONDICIONES ..... 119
1. OBJETIVO DEL DOCUMENTO ..... 119
2. PREMISA ..... 119
3. NOMBRE DEL PROYECTO ..... 119
4. OBJETIVOS DEL PROYECTO PROPUESTO ..... 119
5. NORMAS OFICIALES O CERTIFICACIONES PROPUESTAS ..... 120
6. FOLLETOS, CATÁLOGOS, FOTOGRAFÍAS, MANUALES ENTRE OTROS ..... 120
7. VISITAS A LAS INSTALACIONES ..... 120
8. TIPO DE ABASTECIMIENTO REQUERIDO ..... 120
9. GARANTÍAS ..... 120
10. ACUERDOS DE NIVELES DE SERVICIO PROPUESTOS ..... 121
10.1. PENAS CONVENCIONALES CONSIDERADAS POR OPERBES S.A. DE C.V. ..... 122
10.2. SERVICIOS DE HABILITACIÓN, OPERACIÓN Y TRANSICIÓN ..... 122
10.3. SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA ..... 123
10.4. SERVICIOS DE SEGURIDAD – VERIFICACIÓN/CALIDAD ..... 124
10.5. SERVICIOS DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC) ..... 126
10.6. DEDUCCIONES ..... 126
10.7. DISPONIBILIDAD ..... 127
10.8. TIEMPO PROPUESTO PARA DETECCIÓN Y SOLUCIÓN DE FALLAS PROPUESTOS. 128
10.9. TIEMPO PROPUESTO PARA DETECCIÓN Y MITIGACIÓN DE INCIDENTES ..... 132
10.10. SOLICITUDES DE REQUERIMIENTOS Y CAMBIOS ..... 135
10.11. SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA ..... 139
10.12. SERVICIOS DE SEGURIDAD – VERIFICACIÓN/CALIDAD ..... 140
10.13. SERVICIOS DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC) ..... 144
11. CONDICIONES DE PAGO ..... 149
12. ENTREGABLES ..... 150

12.1. ENTREGABLES GENERALES ..... 150
12.2. ENTREGABLES BAJO DEMANDA ..... 153
12.3. ENTREGABLES PERIÓDICOS ..... 156
13. CONDICIONES DE ACEPTACIÓN DE LOS SERVICIOS ..... 157
14. LUGAR Y HORARIO PARA LA ENTREGA ..... 158
15. CONVENIO DE CONFIDENCIALIDAD Y RESGUARDO DE LA INFORMACIÓN ..... 158
16. PROPIEDAD INTELECTUAL ..... 159
17. MÉTODO DE EVALUACIÓN DE PROPUESTAS ..... 159
18. FUNCIONARIOS PÚBLICOS DE LA DIDT PARTICIPANTES EN EL PROCESO DE CONTRATACIÓN ..... 159
OPERBES S.A. DE C.V. TOMÓ EN CONSIDERACIÓN LOS SIGUIENTES FUNCIONARIOS: ..... 159
19. VIGENCIA DEL CONTRATO ..... 159
20. PLAZO DEL SERVICIO ..... 159
21. ADMINISTRADOR DEL CONTRATO ..... 160
22. MECANISMOS DE CONTROL PARA LA ADMINISTRACIÓN DEL CONTRATO ..... 160
23. MECANISMOS REQUERIDOS AL PROVEEDOR PARA RESPONDER POR DEFECTOS O VICIOS OCULTOS DE LOS BIENES O DE LA CALIDAD DE LOS SERVICIOS ..... 160
24. OTORGAMIENTO DE ANTICIPO ..... 160

ANEXOS
DIVISIÓN DE CONTRATOS

**Propuesta Técnica**

Propuesta técnica que presenta Operbes, S.A. de C.V. en participación en conjunta con Silent4Business, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V. como representante común Operbes, S.A. DE C.V. en adelante referido en la presente propuesta como "Operbes, S.A. de C.V".

## 1. Objetivo del Documento

Operbes S.A. de C.V. Elaborará el presente documento que contiene los requerimientos y las especificaciones técnicas y de calidad, así como el alcance de la adquisición, arrendamiento o servicio de TIC y SI que se pretenda contratar.

Operbes S.A. de C.V. tomó en consideración que el clasificador Único de las Contrataciones Públicas (CUCOP): 31900004 Servicios a centros de datos (hospedaje, electricidad, video vigilancia, monitoreo, aire acondicionado, servidores y otros).

### 1.1. Objetivo General

Operbes S.A. de C.V. tomó en consideración que la convocante requiere ccontar, de manera integrada y unificada, con los servicios administrados mediante dos partidas que garanticen la continuidad operativa, de negocio y de seguridad de la información del IMSS mediante: (1) Toma en operación y transición, (2) servicios de infraestructura que operen, den soporte y mantenimiento a la infraestructura instalada, y que, implementen y gestionen infraestructura para los centros de datos y den la atención a los servicios y aplicaciones con las que cuenta el instituto, (3) servicios que brinden protección a servidores, aplicaciones y bases de datos mediante una solución integral, (4) servicios de seguridad de la información, en materias específicas relacionadas con las tecnologías de la información, comunicaciones y seguridad de la información, incluyendo servicios especializados.

### 1.2. Objetivos Específicos

Operbes S.A. de C.V. tomó en consideración lo siguiente

- Asegurar y proteger la información Institucional.
- Garantizar la continuidad operativa, de negocio y de la seguridad de la información de la Institución, durante la vigencia del presente contrato, especialmente durante la toma de operación y transición del contrato anterior a los servicios propios de SASI 2022-2024.
- Fortalecer la seguridad de la información de la Institución contra amenazas, disminuyendo el riesgo de sufrir incidentes de seguridad, mediante el uso de tecnología de punta para el monitoreo, detección, aseguramiento, contención y respuesta ante ataques que puedan presentarse en la infraestructura de cómputo, sistemas y aplicaciones del IMSS.
- Contar con servicios de infraestructura regulados por niveles de servicio, que: implementen (instalen, migren, habiliten y pongan a punto) los componentes necesarios en los centros de datos y servicios propios del IMSS y que de forma complementaria gestionen (operen, monitoreen, den soporte y mantenimiento preventivo y correctivo) a la correspondiente infraestructura con el propósito de satisfacer las necesidades de: conectividad, comunicación, protección, control y filtrado de la propia Institución, manteniendo la plataforma tecnológica en condiciones óptimas de operación.
- Contar con los servicios de protección de forma unificada e integrada, incluyendo prevención de pérdida de información, protección de cómputo físico o virtual, protección de correo electrónico externo e interno, herramientas de colaboración y trazabilidad, filtrado e inspección de acceso a internet e intranet, mediante una solución integral que permita una gestión consolidada de las

funcionalidades, características y servicios, con el propósito de mantener, asegurar y robustecer el esquema de seguridad del IMSS.

- Contar con servicios de seguridad de la información, que complementen el esquema de seguridad institucional de forma consistente y robusta, con el control, aseguramiento, diagnóstico, pruebas, metodologías, de distintos rubros como el de acceso a cuentas privilegiadas, base de datos, aplicaciones, fuentes múltiples de información para correlación y trazabilidad de eventos, vulnerabilidades, investigación forense y de procesos de seguridad, así como con otros servicios especializados en materia de seguridad y tecnologías de la información.
- Contar con servicios para la gestión del cambio y de soporte extendido que tienen como objetivo coadyuvar en la prestación del resto de los servicios SASI 2022-2024.

## 2. Alcance

Operbes S.A. de C.V. tomó en consideración que el alcance del SASI 2022-2024 incluye:

- Un esquema de servicios de implementación, gestión y monitoreo de la infraestructura física, de seguridad necesaria para integrar los centros de datos mediante una arquitectura flexible y que responda a las necesidades de migración. Este esquema incluye la operación, soporte y mantenimiento de la infraestructura instalada, así como su potencial substitución, con el fin de mantener una plataforma moderna, y uniforme tecnológicamente, que garantice la continuidad operativa, del negocio y de la seguridad de la información del IMSS.
- Un esquema de servicios de protección con una solución integral que incluya: protección de servicios de colaboración internos, correo externo y navegación web, detecte y proteja contra amenazas avanzadas, prevenga la fuga de información y mediante una gestión consolidada.
- Un esquema de servicios de seguridad que complementen el esquema de protección, mediante servicios orientados a: Firewalls, IPS, Filtrado de Contenido, Anti DDoS, Antispam, WAF, DBF, VPN, así como la implementación y administración de nuevos servicios que requiera el instituto, como son análisis de vulnerabilidades, análisis forense, pruebas de penetración, borrado seguro de información, aseguramiento de aplicaciones, ciberinteligencia (ciberseguridad), servicios de protección en redes inalámbricas y seguridad en dispositivos móviles, servicios de gestión y control de acceso para usuarios privilegiados (AAA), servicio de correlación de eventos, servicio de protección de amenazas persistentes avanzadas (APT), servicios de gestión de procesos de seguridad y servicios especializados en materia de seguridad de la información, de este modo, se tiene un esquema de seguridad completo.

## 3. Beneficios

Operbes S.A. de C.V. tomó en consideración que los beneficios que se esperan alcanzar con la prestación de los servicios SASI 2022-2024 se dirigen a garantizar la continuidad de la operación, del negocio y de la seguridad de la información de la propia Institución, fortaleciendo su esquema de infraestructura, comunicaciones, servicios de protección y en servicios especializados en materia de seguridad de la información, contribuyendo al cumplimiento de los objetivos del IMSS; extendiéndose a toda la institución en términos técnicos, protección y servicios especializados como son:

- Contar con una infraestructura física, de seguridad, flexible y escalable; basada en una arquitectura que se adapte oportunamente a las necesidades de migración y a las exigencias para la prestación de los servicios que demanda el IMSS.
- Proporcionar una plataforma tecnológicamente moderna y estandarizada que se mantenga actualizada y en buenas condiciones, para el despliegue oportuno de los servicios que garanticen la continuidad operativa, de negocios y de seguridad de la información del IMSS.
- Contar con un esquema completo de servicios especializados en materia de tecnologías de la información que dé protección tanto a la infraestructura, a los servicios y a los usuarios finales tanto como a aspectos normativos, de procesos, de calidad y de ingeniería entorno a la seguridad de la información.

- Proporcionar los servicios de protección para los usuarios, a través de un esquema desde la red interna y desde la red externa ante los elementos de riesgo y perniciosos que pueden presentarse.
- Garantizar la calidad en la entrega de los servicios de SASI 2022-2024 mediante Acuerdos de Niveles de Servicio elaborados considerando el impacto que genera su no disponibilidad o la no entrega de esos servicios en el esquema de seguridad completo de SASI 2022-2024.

**4. Actualización Tecnológica**

Como parte de su proceso de evolución tecnológica, Operbes S.A. de C.V. tomó en consideración que el IMSS se reserva el derecho de actualizar las especificaciones de infraestructura, de *software* y *hardware* que mantienen los servicios de SASI 2022-2024, toda vez que los activos de infraestructura son susceptibles de integrar mejoras en hardware o software, lo que permite proveer mecanismos de protección adicional conforme la evolución de funcionalides en materia de seguridad o para aquellos que requieran de una sustitución (por falla) o un reajuste. Por lo tanto, Operbes S.A. de C.V. conoce y acepta que el IMSS está en continua evolución tecnológica, por lo que se apegará a ella en todo momento.

Operbes S.A. de C.V. tomó en consideración que como parte de su proceso de evolución tecnológica, el IMSS se reserva el derecho de actualizar las especificaciones de infraestructura, de *software* y *hardware* que mantienen los servicios de SASI 2022-2024, con el objetivo de proteger a la Institución de la obsolescencia, conforme a la misma evolución del mercado observando el mapa de ruta de actualización de los componentes, para los servicios SASI 2022-2024, solicitados o para aquellos que requieran de una sustitución (por falla) o un reajuste. Por lo tanto, Operbes S.A. de C.V. conoce y acepta que el IMSS está en continua evolución tecnológica, por lo que se apegará a ella en todo momento.

Operbes S.A. de C.V. tomó en consideración que por mapa de ruta se refiere a nuevos modelos para reemplazo, y/o sustitución por fin de vida, fin de venta y/o fin de soporte
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 413 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. , tomando en consideración las características del servicio, cumplirá con los mecanismos de seguridad de la información o controles que le establezca la Coordinación de Telecomunicaciones y Seguridad de la Información, con la finalidad de garantizar la conservación, integridad, confiabilidad y disponibilidad de los datos que se encuentran en los sistemas tecnológicos del IMSS una vez que haya iniciado la prestación del servicio, en caso de incumplimiento, Operbes S.A. de C.V. considera lo establecido en el apartado de "Penas Convencionales y Deducciones" de las bases de la licitación.

Operbes S.A. de C.V. efectuará la actualización de cualquier tipo de licencia, componente, dispositivo, parche, arquitectura, etc. siempre y cuando el fabricante de dicho componente haya liberado una versión que lo reemplace por aspectos de seguridad, compatibilidad, fin de soporte, capacidad, error o falla detectada, o similar; con la finalidad de mantener estable y segura la operación de los servicios SASI 2022-2024. Toda actualización o mejora será consultada y aprobada por el IMSS. Estos mecanismos le garantizarán a la institución que, durante toda la vigencia del contrato, dispondrá de los componentes del servicio que incorporan la versión más avanzada de la tecnología validada, probada y liberada por los fabricantes, para satisfacción de las necesidades del servicio SASI 2022-2024.

Operbes S.A. de C.V. tomó en consideración que el licitante adjudicado atenderá a la actualización de hardware, software o licenciamiento cuando se requiera, tanto para aquellos activos que son propiedad del instituto como para aquellos de nueva implementación, esto con base en que los activos de infraestructura estarán disponibles en todo momento a fin de privilegiar su continuidad operativa, lo anterior incluye soporte para nuevas funciones de protección contra ataques, así como el soporte a fallas físicas o lógicas.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 8 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que los plazos para llevar a cabo las actualizaciones tecnológicas de nuevas versiones (*software*) de los componentes relacionados con los servicios de SASI 2022-2024 serán de, por lo menos, seis meses después de su última versión liberada por el fabricante, siempre que el IMSS considere que dicha actualización es conveniente para alcanzar los objetivos de SASI 2022-2024 y del propio IMSS, durante la vigencia del contrato, buscando reducir el riesgo e impacto a la operación, al ejecutar estas actualizaciones siempre se contará con un documento de recomendaciones y riesgos generado por los ingenieros del fabricante al igual se contará con apoyo del centro de asistencia técnica del fabricante durante las ventanas de ejecución de cambios.

ANEXOS
DIVISIÓN DE CONTRATOS

**5. Requerimientos del servicio**

Los Servicios propuestos y que serán parte de la solución propuesta, se desagregan por partida, mismos que incluirán al menos lo siguiente:

## Partida 1

1. **Servicios de Seguridad - Continuidad Operativa**
   (Firewalls, IPS, AntiDDoS, Filtrado Web, Filtrado de correo, Firewall de Aplicaciones WEB, Firewall de base de datos, cifrado de información, Control de Accesos, entre otros.), servicios que cumplirán con los niveles de servicio establecidos para que de manera inmediata y en donde lo requiera el Instituto se continúe con la operación. Estos servicios serán bajo demanda a petición expresa del instituto, así como los tiempos de entrega serán conforme al sitio y dependiendo del tipo de tecnología en una modalidad de alta disponibilidad (HA), así como los niveles de servicios requeridos tanto para la implementación, como la operación, incluyendo los temas de soporte y resolución de problemas e incidentes.

   Operbes S.A. de C.V. tomó en consideración que el cifrado de información se refiere a la característica de cifrado provistas por el Servicio de Redes Privadas Virtuales (VPN) donde se provén conexiones seguras y cifradas entre la red privada de EL INSTITUTO y los usuarios remotos u otra red.
   Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 425 de la empresa Scitum, S.A. de C.V.

2. **Servicios de Seguridad – Verificación y Calidad**
   Consiste en los requerimientos necesarios para que los servicios de calidad de la Seguridad de la Información se continúen, como son, aseguramiento de aplicaciones, cumplimiento normativo, herramientas de seguridad, ciberinteligencia, protección de datos, protección de redes inalámbricas, seguridad de dispositivos móviles y de escritorio, control de acceso a la red, aseguramiento de cuentas privilegiadas, gestión de dominios, administración de certificados digitales, así como los niveles de servicio requeridos en la operación, incluyendo el soporte y resolución de problemas e incidentes.

3. **Servicios del Centro de Operaciones de Seguridad (SOC)**
   Operbes S.A. de C.V. cuenta con un Centro de Operaciones de Seguridad (SOC), que se encuentre físicamente en las instalaciones de Bestel. El objetivo de este centro será la continuidad de la gestión de la seguridad y responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad, la ejecución de actividades de revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, análisis forense, análisis de ciberamenazas avanzadas, auditoria de reglas de acceso, notificación de alertas y vulnerabilidades, así como el establecimiento de acciones de mejora sustentable, la gestión del centro de operaciones de seguridad, parches y actualizaciones de las firmas de las soluciones de seguridad, que opere 7x24x365. El SOC se acredita con presentación de la copia simple del certificado ISO/IEC27001:2013 e ISO/IEC20000-1:2018 vigentes a nombre de Operbes S.A. de C.V. Para dar cumplimiento con este punto favor de referirse al documento llamado "certificados ISO/IEC27001:2013 e ISO/IEC20000-1:2018 vigentes" dentro de la presente propuesta técnica.

   Operbes S.A. de C.V. tomó en consideración que el servicio de SOC solicitado es para dar la continuidad de la gestión de todas las soluciones solicitadas en la partida 1.
   Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 337 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que todos los componentes o infraestructura que se proporcionara a la Convocante para la partida 1 o 2 serán nuevos y de última generación.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 9 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que se proporcionará carta firmada por fabricante indicando que todos los componenentes y/o Infraestructura son nuevos y de última generación. Para dar cumplimiento con este punto favor de referirse al documento llamado "Cartas de fabricante indicando que todos los componentes y/o Infraestructura son nuevos y de última generación " dentro de la presente propuesta técnica.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 9 de la empresa Totalsec, S.A. de C.V.

**6. Requerimientos del Servicio - Especificaciones Técnicas**

**Partida 1.**

**6.1. Servicios de Seguridad – Continuidad Operativa**

**6.1.1. Servicios de Firewall**

**Descripción del servicio**: Operbes S.A. de C.V. tomó en consideración que el instituto requiere de la continuidad operativa del servicio que proporciona la seguridad y protección de control de acceso, filtrado y bloqueo contra ataques dirigidos a las aplicaciones e inspección sobre los paquetes a nivel de aplicación para identificar patrones de tráfico anómalo, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

  Operbes S.A. de C.V. tomó en consideración que es posible hacer la sustitución de los activos de infraestructura de los Servicios de Firewall con los que cuenta hoy en día EL INSTITUTO referidos en el numeral 2. Inventario de Activos de Infraestructura – Servicios de Continuidad del Apéndice "B" por soluciones siempre que cumplan lo descrito en el Apéndice "A" para lo cual LA CONVOCANTE proporcionará un periodo de migración durante el cual se usará el equipamiento existente a fin de garantizar la continuidad operativa, siempre y cuando cumpla con el alcance y los tiempos requeridos por el Instituto.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 557 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que los tiempos de vigencia de la infraestructura se encuentran relacionados con el Fin de vida útil establecidos por los fabricantes, por lo que de ser necesaria una migración esta misma será acordada entre el instituto y el licitante ganador.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 44 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que el licitante ganador contemplará el licenciamiento y soporte con fabricante de los equipos o infraestructura descritos en el Apéndice B, así como la administración
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 10 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que la información señalada en el Apéndice B establece los activos de infraestructura a los cuales se proveerá continuidad operativa, por lo que es necesario que los mismos cuenten con una renovación de licenciamiento independiente al estado actual del servicio. Los detalles de versiones de software serán proporcionados a través de una mesa de trabajo a Operbes S.A. de C.V. en caso de ser el licitante adjudicado.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 12 de la empresa Axtel, S.A.B. de C.V.

- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondientes, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo *stand alone* para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

- Notificar sobre fallas relacionadas con el *hardware* de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*; Dichas evaluaciones se ejecutarán cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el Anexo Técnico de las base de la licitación, tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

  Operbes S.A. de C.V. tomó en consideración que EL INSTITUTO proveerá el espacio en rack, la alimentación eléctrica, las condiciones ambientales (aire acondicionamiento) necesarias para la correcta implementación de los servicios.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 430 de la empresa Scitum, S.A. de C.V.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales *web* u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos firewall para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución estará implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.2. Servicios de Prevención de Intrusos (IPS)**

**Descripción del servicio**: Operbes S.A. de C.V. tomó en consideración que el Instituto requiere de la continuidad operativa del servicio que brinda la protección perimetral basado en firmas y que identifica vulnerabilidades, para contener los intentos de obtener acceso a los recursos o servicios publicados en Internet o Intranet que pudieran afectar la operación de la organización, detectar accesos no autorizados y

prevenir fugas de información, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

  Operbes S.A. de C.V. tomó en consideración que es posible hacer la sustitución de los activos de infraestructura de los Servicios de Prevención de intrusos (IPS) con los que cuenta hoy en día EL INSTITUTO referidos en el numeral 2. Inventario de Activos de Infraestructura – Servicios de Continuidad del Apéndice "B" por soluciones siempre que cumplan lo descrito en el Apéndice "A" para lo cual LA CONVOCANTE proporcionará un periodo de migración durante el cual se usará el equipamiento existente a fin de garantizar la continuidad operativa, siempre y cuando cumpla con el alcance y los tiempos requeridos por el Instituto.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 558 de la empresa Scitum, S.A. de C.V.

  Operbes S.A. de C.V. tomó en consideración que el licitante ganador contemplará el licenciamiento y soporte con fabricante de los equipos o infraestructura descrito en el Apéndice B, así como la administración.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 12 de la empresa Axtel, S.A.B. de C.V.

  Operbes S.A. de C.V. tomó en consideración que la información señalada en el Apéndice B establece los activos de infraestructura a los cuales se proveerá continuidad operativa, por lo que es necesario que los mismos cuenten con una renovación de licenciamiento independiente al estado actual del servicio. Los detalles de versiones de software serán proporcionados a través de una mesa de trabajo a Operbes S.A. de C.V. en caso de ser el licitante adjudicado.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 15 de la empresa Axtel, S.A.B. de C.V.

- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware/software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente.

- Permitir únicamente el tráfico (interno y externo) definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

- Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*; Dichas evaluaciones se ejecutarán cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el Anexo Técnico de las bases de la licitación, tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

  Operbes S.A. de C.V. tomó en consideración que EL INSTITUTO proveerá el espacio en rack, la alimentación eléctrica, las condiciones ambientales (aire acondicionamiento) necesarias para la correcta implementación de los servicios.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 430 de la empresa Scitum, S.A. de C.V.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el Anexo Técnico de las bases de la licitación, tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales *web* u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos IPS para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución estará implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto

- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.3. Servicios de Protección contra Ataques Denegación de Servicio (DDoS)**

**Descripción del servicio**: Operbes S.A. de C.V. tomó en consideración que el Instituto requiere la continuidad operativa del servicio que protege contra los ataques de denegación de servicio distribuido que se encuentre basado en firmas y volúmenes de conexión altos, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.
  Operbes S.A. de C.V. tomó en consideración que es posible hacer la sustitución de los activos de infraestructura de los Servicios de Protección contra ataques denegación de servicio (DDoS) con los que cuenta hoy en día EL INSTITUTO referidos en el numeral 2. Inventario de Activos de Infraestructura – Servicios de Continuidad del Apéndice "B" por soluciones siempre que cumplan lo descrito en el Apéndice "A" para lo cual LA CONVOCANTE proporcionará un periodo de migración durante el cual se usará el equipamiento existente a fin de garantizar la continuidad operativa, siempre y cuando cumpla con el alcance y los tiempos requeridos por el Instituto.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 559 de la empresa Scitum, S.A. de C.V.

  Operbes S.A. de C.V. tomó en consideración que el licitante ganador contemplará el licenciamiento y soporte con fabricante de los equipos o infraestructura descrito en el Apéndice B, así como la administración.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 16 de la empresa Axtel, S.A.B. de C.V.

  Operbes S.A. de C.V. tomó en consideración que la información señalada en el Apéndice B establece los activos de infraestructura a los cuales se proveerá continuidad operativa, por lo que es necesario que los mismos cuenten con una renovación de licenciamiento independiente al estado actual del servicio. Los detalles de versiones de software serán proporcionados a través de una mesa de trabajo a Operbes S.A. de C.V. en caso de ser el licitante adjudicado.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 18 de la empresa Axtel, S.A.B. de C.V.

- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

Operbes S.A. de C.V. tomó en consideración que acepta la convocante que este servicio se presentará de manera hibrida, con la finalidad de poder cubrir la protección de los "Clean pipes", esto dado que una solución on premise no tiene las capacidades de cubrir esta protección.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 276 de la empresa Nelson Morgan Consulting, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que se acepta la prestación de una solución hibrida.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 8 de la empresa Operbes, S.A. de C.V.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondientes, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware o software que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

    - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

    - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del software que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de software y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software; Dichas evaluaciones se ejecutarán cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el Anexo Técnico de las bases de la licitación, tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

  Operbes S.A. de C.V. tomó en consideración que EL INSTITUTO proveerá el espacio en rack, la alimentación eléctrica, las condiciones ambientales (aire acondicionamiento) necesarias para la correcta implementación de los servicios.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 430 de la empresa Scitum, S.A. de C.V.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales *web* u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

  - Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

  - Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos DDoS para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución estará implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

  - Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.4. Servicios de Redes Privadas Virtuales (VPN)**

**Descripción del servicio.** Operbes S.A. de C.V. tomó en consideración que el Instituto requiere la continuidad operativa del servicio de interconexión a través de Internet que permita establecer la comunicación desde localidades remotas para la transferencia de información a través de un canal cifrado, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

Operbes S.A. de C.V. tomó en consideración que es posible hacer la sustitución de los activos de infraestructura de los Servicios de Redes Privadas Virtuales (VPN) con los que cuenta hoy en día EL INSTITUTO referidos en el numeral 2. Inventario de Activos de Infraestructura – Servicios de Continuidad del Apéndice "B" por soluciones siempre que cumplan lo descrito en el Apéndice "A" para lo cual LA CONVOCANTE proporcionará un periodo de migración durante el cual se usará el equipamiento existente a fin de garantizar la continuidad operativa, siempre y cuando cumpla con el alcance y los tiempos requeridos por el Instituto.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 560 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que el licitante ganador contemplará el licenciamiento y soporte con fabricante de los equipos o infraestructura descrito en el Apéndice B, así como la administración.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 19 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que la información señalada en el Apéndice B establece los activos de infraestructura a los cuales se proveerá continuidad operativa, por lo que es necesario que los mismos cuenten con una renovación de licenciamiento independiente al estado actual del servicio. Los detalles de versiones de software serán proporcionados a través de una mesa de trabajo a Operbes S.A. de C.V. en caso de ser el licitante adjudicado.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 21 de la empresa Axtel, S.A.B. de C.V.

- Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea requerido por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo independiente (*stand alone)* para la administración de los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

  - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del software que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones se ejecutarán cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el Anexo Técnico de las bases de la licitación, tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
  Operbes S.A. de C.V. tomó en consideración que EL INSTITUTO proveerá el espacio en rack, la alimentación eléctrica, las condiciones ambientales (aire acondicionamiento) necesarias para la correcta implementación de los servicios.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 430 de la empresa Scitum, S.A. de C.V.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las

mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos VPN para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución estará implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.5. Servicios de Filtrado de Contenido Web**

**Descripción del servicio.** Operbes S.A. de C.V. tomó en consideración que el Instituto requiere la continuidad operativa del servicio de filtrado de contenido Web mediante políticas de acceso que permite controlar y filtrar la utilización del servicio de acceso a Internet, en función de roles y perfiles, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

  Operbes S.A. de C.V. tomó en consideración que es posible hacer la sustitución de los activos de infraestructura de los Servicios de Filtrado de Contenido Web con los que cuenta hoy en día EL INSTITUTO referidos en el numeral 2. Inventario de Activos de Infraestructura – Servicios de Continuidad del Apéndice "B" por soluciones siempre que cumplan lo descrito en el Apéndice "A" para lo cual LA CONVOCANTE proporcionará un periodo de migración durante el cual se usará el equipamiento existente a fin de garantizar la continuidad operativa, siempre y cuando cumpla con el alcance y los tiempos requeridos por el Instituto.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 561 de la empresa Scitum, S.A. de C.V.

  Operbes S.A. de C.V. tomó en consideración que el licitante ganador contemplará el licenciamiento y soporte con fabricante de los equipos o infraestructura descrito en el Apéndice B, así como la administración.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 22 de la empresa Axtel, S.A.B. de C.V.

  Operbes S.A. de C.V. tomó en consideración que la información señalada en el Apéndice B establece los activos de infraestructura a los cuales se proveerá continuidad operativa, por lo que es necesario que los mismos cuenten con una renovación de licenciamiento independiente al estado actual del servicio. Los detalles de versiones de software serán proporcionados a través de una mesa de trabajo a Operbes S.A. de C.V. en caso de ser el licitante adjudicado.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 24 de la empresa Axtel, S.A.B. de C.V.

- Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

  - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del software que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones se ejecutarán cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

  Operbes S.A. de C.V. tomó en consideración que EL INSTITUTO proveerá el espacio en rack, la alimentación eléctrica, las condiciones ambientales (aire acondicionamiento) necesarias para la correcta implementación de los servicios.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 430 de la empresa Scitum, S.A. de C.V.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos de Filtrado de Contenido Web para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución estará implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.6. Servicios de Filtrado de Contenido de Correo (Antispam)**

**Descripción del servicio.** Operbes S.A. de C.V. tomó en consideración que el Instituto requiere la continuidad operativa de un servicio para analizar correos electrónicos de entrada y salida con el objetivo de bloquear aquellos que sean clasificados como spam, malware, phishing y con contenido malicioso, entre otros, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

Operbes S.A. de C.V. tomó en consideración que el servicio de correo electrónico es hibrido.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 25 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que la cantidad de buzones a proteger es de al menos 80,000 buzones.

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 26 de la empresa Axtel, S.A.B. de C.V.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

  Operbes S.A. de C.V. tomó en consideración que es posible hacer la sustitución de los activos de infraestructura de los Servicios de Filtrado de Contenido de Correo (Antispam) con los que cuenta hoy en día EL INSTITUTO referidos en el numeral 2. Inventario de Activos de Infraestructura – Servicios de Continuidad del Apéndice "B" por soluciones siempre que cumplan lo descrito en el Apéndice "A" para lo cual LA CONVOCANTE proporcionará un periodo de migración durante el cual se usará el equipamiento existente a fin de garantizar la continuidad operativa, siempre y cuando cumpla con el alcance y los tiempos requeridos por el Instituto.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 562 de la empresa Scitum, S.A. de C.V.

  Operbes S.A. de C.V. tomó en consideración que el licitante ganador contemplará el licenciamiento y soporte con fabricante de los equipos o infraestructura descrito en el Apéndice B, así como la administración.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 27 de la empresa Axtel, S.A.B. de C.V.

  Operbes S.A. de C.V. tomó en consideración que la información señalada en el Apéndice B establece los activos de infraestructura a los cuales se proveerá continuidad operativa, por lo que es necesario que los mismos cuenten con una renovación de licenciamiento independiente al estado actual del servicio. Los detalles de versiones de software serán proporcionados a través de una mesa de trabajo a Operbes S.A. de C.V. en caso de ser el licitante adjudicado.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 29 de la empresa Axtel, S.A.B. de C.V.

- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Proteger el correo electrónico de entrada y salida, así como la reputación del direccionamiento IP que se utiliza para generar esta comunicación en Internet, para lo cual incluirá, un servicio de protección a través de los activos de infraestructura existente así como un mecanismo de sanitización en la nube de Internet que prevea una doble capa de verificación sobre correos anómalos o no deseados (spam), con virus o malware.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

    - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

    - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones se ejecutarán cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el Anexo Técnico de las bases de la licitación tales como, componentes

habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

Operbes S.A. de C.V. tomó en consideración que EL INSTITUTO proveerá el espacio en rack, la alimentación eléctrica, las condiciones ambientales (aire acondicionamiento) necesarias para la correcta implementación de los servicios.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 430 de la empresa Scitum, S.A. de C.V.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos Antispam para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución estará implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.7. Servicios de Firewall Especializado en Servicios Web (WAF)**

**Descripción del servicio.** Operbes S.A. de C.V. tomó en consideración que el Instituto requiere la continuidad del servicio de protección, prevención y control de ataques para aplicativos web expuestos en Internet/Intranet, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

  Operbes S.A. de C.V. tomó en consideración que el licitante ganador contemplará el licenciamiento y soporte con fabricante de los equipos o infraestructura descrito en el Apéndice B, así como la administración.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 30 de la empresa Axtel, S.A.B. de C.V.

  Operbes S.A. de C.V. tomó en consideración que la información señalada en el Apéndice B establece los activos de infraestructura a los cuales se proveerá continuidad operativa, por lo que es necesario que los mismos cuenten con una renovación de licenciamiento independiente al estado actual del servicio. Los detalles de versiones de software serán proporcionados a través de una mesa de trabajo a Operbes S.A. de C.V. en caso de ser el licitante adjudicado.

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 32 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que es posible hacer la sustitución de los activos de infraestructura de los Servicios de Firewall Especializado en servicio Web (WAF) con los que cuenta hoy en día EL INSTITUTO referidos en el numeral 2. Inventario de Activos de Infraestructura – Servicios de Continuidad del Apéndice "B" por soluciones siempre que cumplan lo descrito en el Apéndice "A" para lo cual LA CONVOCANTE proporcionará un periodo de migración durante el cual se usará el equipamiento existente a fin de garantizar la continuidad operativa, siempre y cuando cumpla con el alcance y los tiempos requeridos por el Instituto.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 563 de la empresa Scitum, S.A. de C.V.

- Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

  - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del software que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones se ejecutarán cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el Anexo Técnico de las bases de la licitación tales como, componentes habilitadores de comunicaciones entre redes; cableado eléctrico y de datos, montaje en racks, entre otros.

  Operbes S.A. de C.V. tomó en consideración que EL INSTITUTO proveerá el espacio en rack, la alimentación eléctrica, las condiciones ambientales (aire acondicionamiento) necesarias para la correcta implementación de los servicios.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 430 de la empresa Scitum, S.A. de C.V.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos WAF para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución estará implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.8. Servicios de Firewall especializado en Base de Datos (DBF)**

**Descripción del servicio**. Operbes S.A. de C.V. tomó en consideración que el Instituto requiere la continuidad operativa del servicio de protección a las instancias de bases de datos en tiempo real, así como el monitoreo del tráfico de base de datos con la finalidad de realizar la detección de ataques avanzados, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

Operbes S.A. de C.V. tomó en consideración que para el correcto dimensionamiento en licenciamiento se considera al menos 10 instancias de bases de datos a proteger y 10 servidores.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 493 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que las instancias y servidores son adicionales a la base ya instalada.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 25 de la empresa Totalsec, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que el sitio donde se instalará el servicio de Firewall especializado en base de Datos (DBF) es Morelia, Michoacán.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 494 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que se proporcionará mínimo 1 y máximo 2 para el centro de datos de Morelia Michoacán, información que se encuentra descrita en el apéndice A.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 495 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que se requieren interfaces 4 x 10G SR
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 496 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que es necesario identificar las actividades de datos incluso si son generadas por servidores de aplicaciones.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 497 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que el servicio será capaz de brindar visibilidad y trazabilidad sobre las peticiones hacia las bases de datos.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 498 de la empresa Scitum, S.A. de C.V.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

Operbes S.A. de C.V. tomó en consideración que es posible hacer la sustitución de los activos de infraestructura de los Servicios de Firewall Especializado en base de datos (DBF) con los que cuenta hoy en día EL INSTITUTO referidos en el numeral 2. Inventario de Activos de Infraestructura – Servicios de Continuidad del Apéndice "B" por soluciones siempre que cumplan lo descrito en el Apéndice "A" para lo cual LA CONVOCANTE proporcionará un periodo de migración durante el cual se usará el equipamiento existente a fin de garantizar la continuidad operativa, siempre y cuando cumpla con el alcance y los tiempos requeridos por el Instituto.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 564 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que el licitante ganador contemplará el licenciamiento y soporte con fabricante de los equipos o infraestructura descrito en el Apéndice B, así como la administración.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 33 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que la información señalada en el Apéndice B establece los activos de infraestructura a los cuales se proveerá continuidad operativa, por lo que es necesario que los mismos cuenten con una renovación de licenciamiento independiente al estado actual del servicio. Los detalles de versiones de software serán proporcionados a través de una mesa de trabajo a Operbes S.A. de C.V. en caso de ser el licitante adjudicado.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 35 de la empresa Axtel, S.A.B. de C.V.

- Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (Base de datos), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las zonas de servidores.

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

    - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

    - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones se ejecutarán cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

  Operbes S.A. de C.V. tomó en consideración que EL INSTITUTO proveerá el espacio en rack, la alimentación eléctrica, las condiciones ambientales (aire acondicionamiento) necesarias para la correcta implementación de los servicios.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 430 de la empresa Scitum, S.A. de C.V.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos DBF para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución estará implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.9. Servicios de Gestión Unificada de Amenazas (UTM)**

**Descripción del servicio.** Operbes S.A. de C.V. tomó en consideración que el Instituto requiere la continuidad operativa del servicio de protección perimetral especializada en control de acceso, prevención de intrusos, filtrado de contenido Web y VPN, para control de tráfico y detección de actividad anómala, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.

  Operbes S.A. de C.V. tomó en consideración que es posible hacer la sustitución de los activos de infraestructura de los Servicios de Gestión Unificada de Amenazas (UTM) con los que cuenta hoy en día EL INSTITUTO referidos en el numeral 2. Inventario de Activos de Infraestructura – Servicios de Continuidad del Apéndice "B" por soluciones siempre que cumplan lo descrito en el Apéndice "A" para lo cual LA CONVOCANTE proporcionará un periodo de migración durante el cual se usará el equipamiento existente a fin de garantizar la continuidad operativa, siempre y cuando cumpla con el alcance y los tiempos requeridos por el Instituto.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 565 de la empresa Scitum, S.A. de C.V.

  Operbes S.A. de C.V. tomó en consideración que el licitante ganador contemplará el licenciamiento y soporte con fabricante de los equipos o infraestructura descrito en el Apéndice B, así como la administración.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 36 de la empresa Axtel, S.A.B. de C.V.

  Operbes S.A. de C.V. tomó en consideración que la información señalada en el Apéndice B establece los activos de infraestructura a los cuales se proveerá continuidad operativa, por lo que es necesario que los mismos cuenten con una renovación de licenciamiento independiente al estado actual del servicio. Los detalles de versiones de software serán proporcionados a través de una mesa de trabajo a Operbes S.A. de C.V. en caso de ser el licitante adjudicado.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 38 de la empresa Axtel, S.A.B. de C.V.

- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.

- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.

- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

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

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

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

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

    - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

    - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros,

mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones se ejecutarán cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el Anexo Técnico de las bases de la licitación, tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

  Operbes S.A. de C.V. tomó en consideración que EL INSTITUTO proveerá el espacio en rack, la alimentación eléctrica, las condiciones ambientales (aire acondicionamiento) necesarias para la correcta implementación de los servicios.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 430 de la empresa Scitum, S.A. de C.V.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos UTM para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución estará implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.10. Servicio de Correlación de Eventos**

**Descripción del servicio.** Operbes S.A. de C.V. tomó en consideración que el Instituto requiere de un servicio de seguridad que administre, analice, explote, emplee y aproveche las bitácoras de los dispositivos de seguridad con la finalidad de conocer exactamente qué pasa en distintos puntos de la red de forma centralizada y eliminar falsos positivos generados, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

- Proporcionar activos de infraestructura nuevos de última generación y dedicados exclusivamente para las necesidades del Instituto.

  Operbes S.A. de C.V. tomó en consideración que la cantidad de EPS a correlacionar en el servicio de correlación de eventos al menos 10.000 eventos por segundo.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 39 de la empresa Axtel, S.A.B. de C.V.
  Operbes S.A. de C.V. tomó en consideración que el tiempo de resguardo de los eventos o bitácoras será de al menos 6 meses, que estarán normalizadas.

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 40 de la empresa Axtel, S.A.B. de C.V.

- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).

- Integrar activos de infraestructura de propósito específico (*appliances* o servidores físicos) con capacidades de expansión bajo demanda conforme lo dispuesto en el Apéndice A.

- Definir en conjunto con el Instituto la estrategia de habilitación de los nuevos activos de infraestructura para correlación de eventos en la arquitectura de seguridad y comunicaciones.

- Ejecutar todas las tareas necesarias para la instalación del equipo en los Centro de Datos correspondientes, o en su caso, aquella otra localidad donde le sea requerido por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.

- Integrar cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo independiente (*stand alone)* para la administración de todos los dispositivos, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Asegurar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente.

- Permitir únicamente la correlación definida por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión vía syslog con otras redes o nubes.

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

- Monitorear los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

- Notificar sobre fallas relacionadas con el *hardware* de los activos de infraestructura provisto a través del servicio.

- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, Operbes S.A. de C.V. presentará la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.

- Integrar el licenciamiento del *software* que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) que permitan identificar, entre otros: mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Dichas evaluaciones se ejecutarán cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en software que permitan acceder a las mismas (*aplicaciones* cliente-servidor, portales web u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos del Correlacionador de Eventos para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución estará implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.1.11. Servicio de Protección de Amenazas Persistentes Avanzadas (APT)**

**Descripción del servicio**. Operbes S.A. de C.V. tomó en consideración que el Instituto requiere la habilitación de un servicio que le permita tener la capacidad de protegerse de amenazas avanzadas que se encuentren activas en la organización y que hayan podido sobrepasar los controles de seguridad existentes, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

- Proporcionar activos de infraestructura nuevos de última generación y dedicados exclusivamente para las necesidades del Instituto.
  Operbes S.A. de C.V. tomó en consideración que la cantidad de troughput a inspeccionar será al menos 5 Gbps.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 41 de la empresa Axtel, S.A.B. de C.V.

  Operbes S.A. de C.V. tomó en consideración que los 5 Gbps, se considera por cada equipo requerido.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 10 de la empresa Scitum, S.A. de C.V.

  Operbes S.A. de C.V. tomó en consideración que la cantidad de puertos y la velocidad que se proporcionara de la solución es 4xGE y 4 x10GE(SPF).
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 42 de la empresa Axtel, S.A.B. de C.V.

  Operbes S.A. de C.V. tomó en consideración que los 4 puertos 1GE y 4 puertos x10GE(SPF) , se considera por cada equipo requerido.

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 11 de la empresa Scitum, S.A. de C.V.

- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).

- Integrar activos de infraestructura de propósito específico (*appliances*) con capacidades de expansión bajo demanda, pudiendo ser estas últimas instancias virtuales, conforme lo dispuesto en el Apéndice A.

  Operbes S.A. de C.V. tomó en consideración que en virtud de que la protección de Anti-DDoS es sumamente demandante en cuanto al procesamiento de tráfico y considerando el tamaño y demanda del propio INSTITUTO, que además de solicitar infraestructura de propósito específico (Appliances) sean soluciones basadas en Hardware y no como instancias virtuales a fin no comprometer la protección Anti-DDoS del INSTITUTO, siempre y cuando se cumplan con los niveles de servicio.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 432 de la empresa Scitum, S.A. de C.V.

  Operbes S.A. de C.V. tomó en consideración que se aceptan propuestas de servicio de protección DDoS que sean capaces de mitigar ataques incluso antes de que afecten a la infraestructura de propósito específico.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 24 de la empresa Totalsec, S.A. de C.V.

- Definir en conjunto con el Instituto la estrategia de habilitación de los nuevos activos de infraestructura para Amenazas Persistentes Avanzadas en la arquitectura de seguridad y comunicaciones.

- Ejecutar las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.

- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware/software* que integran el servicio sin un control de cambios autorizado por este último.

- Integrar cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.

- Asegurar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente.

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

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

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

- Monitorear los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.

- Notificar sobre fallas relacionadas con el *hardware* de los activos de infraestructura provisto a través del servicio.

- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, Operbes S.A. de C.V. presentará la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.

- Integrar el licenciamiento del *software* que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.

- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) que permitan identificar, entre otros: mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Dichas evaluaciones se ejecutarán cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales *web* u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos del servicio de Amenazas Persistentes Avanzadas para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución estará implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice A.

**6.2. Servicios de Seguridad – verificación y calidad**

Operbes S.A. de C.V. tomó en consideración que el Instituto requiere continuar con la prestación de servicios bajo demanda durante la vigencia del contrato y que a través de este se definan, identifiquen, clasifiquen y prioricen las debilidades de las aplicaciones que proporcionan una evaluación de las amenazas previsibles,

que permitan reaccionar de manera apropiada, así como robustecer la confidencialidad, integridad y disponibilidad de la información, atendiendo a las necesidades operativas del IMSS.

### 6.2.1. Servicios de Borrado Seguro de Información

**Descripción del servicio.** Operbes S.A. de C.V. dará continuidad a la solución de borrado seguro de información, para los dispositivos tales como computadoras personales, laptops, servidores, unidades de almacenamiento fijas, removibles, externos y cualquier otro que el Instituto determine, con el fin de evitar la pérdida y dispersión de información propiedad de este; lo anterior aplicará cuando sean retirados dichos dispositivos por motivos de conclusión de contrato, obsolescencia, falla, baja y/o reasignación, entre otros. Para tal efecto se requiere la renovación del derecho de uso y soporte técnico de los productos de *software* de borrado seguro, así como, la actualización de dicho licenciamiento, actualizaciones (*updates* y *upgrades*) que permitan garantizar la confidencialidad de la información propiedad del Instituto, cumpliendo con lo establecido en la legislación vigente y aplicable relacionada con los derechos de autor.

Operbes S.A. de C.V. tomó en consideración que cuando se refiere a "cualquier otro que el Instituto determine" estos pueden ser borrado de base de datos, LUN´s, contenedores, máquinas virtuales, cintas LTO.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 446 de la empresa Scitum, S.A. de C.V.

Los servicios proporcionados por Operbes S.A. de C.V. , así como las entregas de información requeridas en el presente documento, se apegará a la normativa vigente aplicable para dichos servicios y soluciones, por lo que Operbes S.A. de C.V. cumplir con las siguientes especificaciones funcionales mínimas.

- Integrar todas aquellas renovaciones que sean necesarias durante la vigencia de los servicios.

  Operbes S.A. de C.V. tomó en consideración que el nombre del fabricante y software utilizado para llevar a cabo el borrado Seguro es Blanco Technology Group.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 44 de la empresa Axtel, S.A.B. de C.V.

- Garantizar que las herramientas de borrado seguro cuenten con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios del servicio correspondiente.

- Permitirá realizar borrados completos en medios de almacenamiento dispuestos en activos de infraestructura como: equipos de cómputo (de escritorio y portátil), equipos de propósito específico (*appliance*), servidores físicos o virtuales, derivado de la sustitución, migraciones o retiro por finalización del contrato.

- Asegurará que los datos no puedan ser recuperados, basándose en al menos los siguientes estándares internacionales.

  - HMG Infosec Standard 5 (baseline and enhanced)
  - Opnavinst 5239.1A
  - Extended NIST 800-88
  - DoD 5220.22-M
  - ISO-IEC 15408
  - ECE y BSI/VSITR

- Borrado de Discos duros IDE/ATA, SCSI, SAS, USB, SATA, SSD, Fiber Channel y FireWire, de estado sólido y mecánicos de cualquier tamaño.
- Brindará la destrucción local y/o remota en múltiples dispositivos de almacenamiento.
- Posibilitará el desmontaje RAID (SCSI).
- Permitirá el borrado y detección de zonas bloqueadas / ocultas (DCO, HPA).
- Generará certificados de borrado infalsificables que ofrezcan protección ante cualquier instancia legal, en donde se incluya el resultado del proceso de borrado, fecha, hora, los datos del equipo, el detalle del dispositivo de almacenamiento borrado.
- Emitirá una firma electrónica para la autenticación de la integridad del reporte de sanitización emitido por el *software* de borrado.
- La solución se ejecutará sin importar de que sistema operativo se trate.
- El reporte que generé la solución será exportado a un medio de almacenamiento como USB o disco duro.
- El servicio de borrado seguro esta provisto mediante un proceso o flujo operativo, el cual contemplará entre otros, los siguientes puntos:

  - Solicitud de borrado.
  - Identificación del medio de borrado.
  - Definición de fecha de borrado.
  - Flujos operativos para la autorización de borrado o destrucción.
  - Como referencia, se muestran los insumos a ser atendidos

| DISPOSITIVOS |
|---|
| **Derecho Uso de Licencias y Soporte Técnico** |
| PC y Laptops |
| Servidores |
| Máquinas Virtuales y Unidades Lógicas |
| Archivos, carpetas, bases de datos |
| Console Management |
| **Servicio de Soporte Técnico Especializado** |
| Disco Duro, PC, Laptops, Disco Duro Servidor y Disco Duro Storage |
| Borrado de Bases de Datos, LUN's y Contenedores |
| Borrado de Máquinas Virtuales |
| Degaussing Discos Duros, SSD y Cintas LTO |

Operbes S.A. de C.V. tomó en consideración que el instituto realiza borrado seguro de información bajo demanda conforme las especificaciones descritas en el Anexo Técnico de las bases de la licitación, por lo que no existe un inventario establecido que determine las marcas, modelos y capacidad de disco duros

Respecto a los tipos de disco se tienen contemplados al menos:

IDE, ATA, SAS, SCSI

Operbes S.A. de C.V. tomó en consideración que respecto a los sistemas operativos se tienen contemplados al menos:

- Windows 7, Windows 10, Windows Server 2012, Windows Server 2016, Linux Redhat Enterprise 8.0 o mayor.
- Operbes S.A. de C.V. tomó en consideración que respecto a los virtualizadores se tienen contemplados al menos:
  VMWare, KVM
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 45 de la empresa Axtel, S.A.B. de C.V.

- La continuidad del servicio considerará que los usuarios puedan acceder a las consolas de administración de la solución para la gestión, administración, supervisión y operación, todo ello con el fin de habilitar las funcionalidades operativas para realizar el borrado seguro de manera descentralizada (en oficinas remotas).

**6.2.2. Servicio de Gestión de Dominios**

**Descripción del servicio**. Continuidad operativa del servicio que permita registrar ante las instancias certificadas por el NIC, los dominios que requiera el Instituto y su correcta gestión, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

- Registro – Llevar a cabo el seguimiento correspondiente ante las instancias certificadoras
  - Revisar y dar seguimiento a el nombre de domino acordado con el personal designado por el Instituto
  - Revisar que no se encuentre duplicado o usado por ningún tercero

- Alojamiento – Dar seguimiento al alojamiento de dicho dominio
  - Actualización de las directivas de seguridad.
  - Continuidad al mantenimiento requerido

Operbes S.A. de C.V. continuará con la gestión y los pagos que correspondan derivados del registro, cambio de dominio o proveedor sin costo adicional para el Instituto.

Operbes S.A. de C.V. tomó en consideración que la cantidad de dominios al menos será 4 dominios.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 306 de la empresa Operbes, S.A. de C.V.

**6.2.3. Servicio de Certificados Digitales SSL**
**Descripción del Servicio**. Operbes S.A. de C.V. proporcionará la continuidad del servicio que permite contar con certificados SSL para la protección de las páginas web del Instituto, durante la vigencia del contrato, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

- Validación de dominios
- Cifrado SSL de al menos 256 bits
- No debe de ser auto firmado, sino emitido por una instancia certificadora válida (tercero confiable)
- El tiempo de emisión cumplirá con los niveles de servicios establecidos para hacerlo llegar al personal del Instituto vía correo electrónico
- Operbes S.A. de C.V. se hará cargo de la gestión en cuanto a pagos de derecho y cualquier cargo derivado de contar con el o los certificados.
- Los certificados serán al menos de los siguientes tipos:
  - Certificados SSL con validación de dominio (DV SSL)
    - Certificado para un solo dominio
    - Certificado para múltiples dominios (SAN)
    - Certificados comodines (wildcard)

**6.2.4. Servicios de Ciberinteligencia (Ciberseguridad)**

**Descripción del servicio.** Operbes S.A. de C.V. tomó en consideración que el Instituto requiere de un servicio con inteligencia accionable que le permita actuar oportunamente para protegerse y minimizar amenazas o ataques informáticos detectados a través de campañas y operaciones identificadas, al mismo tiempo que pueda ordenar investigaciones de acuerdo a sus necesidades, por lo que Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.
Operbes S.A. de C.V. tomó en consideración que el Instituto será responsable de promover con las entidades correspondientes las acciones de baja de portales.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 4 de la empresa Operbes, S.A. de C.V.

- Detectar posible venta de información confidencial del Instituto en mercados negros.
- Dar seguimiento a grupos hacktivistas y del cibercrimen nacionales y extranjeros que puedan representar una amenaza para el Instituto.
- Poder infiltrarse en canales de IRC donde se perpetren y difundan campañas de ataques informáticos que puedan afectar al Instituto.
- Monitorear foros y comunidades tanto de redes abiertas como de la Red Onion/TOR donde se perpetren y difundan campañas de ataques informáticos que pudieran representar un riesgo para el Instituto.
- Poder monitorear las noticias tanto nacionales como extranjeras tanto en la red abierta como en la Deep Web para la colección de inteligencia táctica, que permita al Instituto tomar acciones preventivas adicionales para la protección de infraestructura susceptible de un ataque informático.

  Operbes S.A. de C.V. tomó en consideración que se refiere sólo al monitoreo de noticias que representen una amenaza cibernética crítica para EL INSTITUTO.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 544 de la empresa Scitum, S.A. de C.V.

- Colectar, a través de un cuestionario especializado, los elementos que provean la información necesaria para realizar el análisis de la situación global del Instituto, así como generar los perfiles de investigación a ser utilizados para los servicios permanentes.
- A través de un cuestionario en esta etapa se recopilará la siguiente información:
  - Páginas publicadas.
  - Historial de amenazas de seguridad experimentadas por el Instituto.
  - Sistemas críticos consultados por usuarios externos.
  - Lista de activos críticos y su atracción o valor para el ciber-crimen.
  - Contactos para la elaboración de la matriz de escalación.
  - Datos para la elaboración de la declaración de trabajo (SOW por sus siglas en inglés).
- Realizar un análisis de la situación global del instituto, una vez teniendo el contexto de su entorno e identificando el tipo de exposición y amenazas que podrían impactarle de acuerdo al acontecer local y las amenazas globales del sector en el que se desenvuelve.

- Generación de perfiles de investigación con la información recabada. Dicho perfil de investigación será utilizado durante la vigilancia de Ciberinteligencia, el cual incluye lo siguiente:

  - Perfiles virtuales a emplear.
  - Definición de fuentes asociadas a los perfiles virtuales utilizados en el monitoreo.

- Determinar los umbrales para los eventos que dispararán las alertas que se deberán de notificar hacia la matriz de notificación definida en conjunto con el Instituto para los servicios como "Vigilancia Permanente de Ciberinteligencia".

- Mantener supervisión de los correos/sitios de phishing y direcciones IP dudosas que le comparta el instituto con el fin de realizar un análisis de los mismos. De manera adicional se realizará vigilancia en el ciberespacio las 24 horas del día los 365 días del año, sobre redes sociales, Darknet, buscadores de internet de las cosas, entre otras fuentes, para ello se colectará inteligencia empleando técnicas de OSINT (Open Source Intelligence) como líneas de tiempo y mapas de conexiones, Virtual HUMINT donde se emplean la infiltración de perfiles virtuales.

  Operbes S.A. de C.V. tomó en consideración que el análisis de los correos será bajo demanda y sólo de aquellos que hayan burlado las herramientas de detección y protección propias del Servicios de Filtrado de Contenido de Correo (Antispam).
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 546 de la empresa Scitum, S.A. de C.V.

- Identificar campañas para ataques específicos, venta de información, infraestructura vulnerable expuesta a través de internet, relaciones entre perfiles, grupos privados de facebook, entre otros.

- Realizar esta evaluación en cualquiera de los siguientes casos:

  - Durante la vigilancia de Ciberinteligencia, al encontrarse algún hallazgo que represente realmente una amenaza para el Instituto, se realizará una notificación inicial con la finalidad de que el Instituto pueda tomar las líneas de acción necesarias para mitigar la amenaza descubierta.
  - Cuando se solicite el análisis de sitios dedicados al phishing, correos que contengan phishing o direcciones IP.
  - Durante la elaboración del análisis del comportamiento de los grupos hacktivistas.
  - Durante el análisis de las direcciones IP, producto de ataques de denegación de servicios que haya experimentado el Instituto.

- Realizar un análisis correlacionando toda la información recolectada por las herramientas y la situación general alrededor del evento, a partir de este análisis emitirá un dictamen hacia el instituto con inteligencia accionable, táctica u operativa según corresponda, en un plazo no mayor a 24 horas después de la detección de cualquiera de los siguientes eventos:

  - Declaración de posibles ataques de denegación de servicio por parte de grupos hacktivistas o del cibercrimen.
  - Defacements.
  - Fuga de información confidencial del Instituto hacia sitios públicos.
  - Malware dirigido.
  - Phishing detectado en parking domains.
  - Indicios de amenazas o ataques informáticos sobre el Instituto.
  - Existencia de campañas (conjunto de acciones para perpetrar un ataque informático) en contra del Instituto.
  - Venta o publicación de información sensible del Instituto en la Darknet.

- Publicación de información confidencial de personal del Instituto como usuarios y contraseñas.
- Nuevos esquemas de fraude detectados en otros organismos del sector.

- Para cualquier otro tipo de evento distinto a los listados solo se realizará la notificación inicial.

- Se generará el proceso de inteligencia accionable en cualquiera de los siguientes casos:
  - Cuando se detecte que un ataque ya sucedió y tuvo un impacto en el Instituto, para lo cual se emitirán recomendaciones hacia el Instituto.
  - En los casos donde se realice el análisis a petición del Instituto de sitios o correos relacionados con phishing así como direcciones IP, se generará a partir de los hallazgos identificados inteligencia accionable donde se incluirá detalles sobre los sitios, direcciones IP, artefactos maliciosos, entre otros, al igual que sobre los reportes generados como parte de los servicios.

- Realizar el análisis de hasta 50 direcciones IP que el Instituto considere dudosas por mes, con el objetivo de analizarlas en búsqueda de información relacionada con ataques, además de determinar si éstas han realizado intrusiones a otros organismos de similares características a las del Instituto, si forman parte de una botnet, han sufrido un defacement, o bien forman parte de alguna campaña en particular.
  Operbes S.A. de C.V. tomó en consideración que el análisis de hasta 50 direcciones IP será bajo demanda bajo solicitud de EL INSTITUTO ya que no se esperan que mensualmente se mantenga esa cantidad de activos en riesgo.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 547 de la empresa Scitum, S.A. de C.V.

- Analizar el comportamiento del hacktivismo en México y su relación con otros grupos, incluyendo el detalle de las operaciones del mes en curso, sus objetivos y el impacto de las mismas, así como recomendaciones para protegerse ante las nuevas operaciones esperadas.
  Operbes S.A. de C.V. tomó en consideración que el análisis de comportamiento del hacktivismo forma parte del
  monitoreo permanente de ciberinteligencia
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 548 de la empresa Scitum, S.A. de C.V.

- Analizar hasta 3 correos electrónicos o sitios al mes, con los cuales se realizarán entre otras las siguientes acciones:

  - Identificación de los encabezados y análisis del malware en el contenido.
  - Extracción de datos como dominios y direcciones IP, mismas que serán analizadas en una plataforma de "Inteligencia sobre Amenazas" para determinar el riesgo que representa el Phishing para el Instituto.

  Operbes S.A. de C.V. tomó en consideración que el análisis de hasta 3 correos electrónicos o sitios al mes será bajo demanda bajo solicitud de EL INSTITUTO ya que no se esperan que mensualmente se mantenga esa cantidad de elementos potencialmente dañinos o en riesgo.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 549 de la empresa Scitum, S.A. de C.V.

**6.2.5. Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos Móviles.**

**Descripción del servicio.** Operbes S.A. de C.V. tomó en consideración que el Instituto requiere un servicio de protección en redes inalámbricas específicas que permitan colocar controles que garanticen y protejan la información producida internamente y recibida a través de los recursos de redes inalámbricas (WLAN), contra ataques generales que buscan aprovechar esta modalidad para infiltrarse en la red de comunicaciones del Instituto, así mismo se requiere un servicio de protección de dispositivos móviles, que prevenga el robo o sustracción de información considerando para lo anterior, la administración de políticas y el cumplimiento de operación en los dispositivos móviles, Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

Operbes S.A. de C.V. tomó en consideración que el servicio de protección de redes inalámbricas requiere un servicio tipo MDM para dar cumplimiento a lo establecido en el numeral 6.2.5 del anexo técnico de la Convocatoria.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 49 de la empresa Axtel, S.A.B. de C.V.

- Garantizar que las herramientas propuestas para el servicio cuenten con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios con el que cuente el servicio correspondiente.

- Integrar el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.

- Proteger contra ataques informáticos comunes a la red inalámbrica (WLAN).

- Actualizar y mejorar los procesos que permitan la autenticación de usuarios internos.

- Cifrado TKIP y AES basado en *hardware*.

- Tener la funcionalidad de WIPS en tiempo real (prevención de intrusiones inalámbricas).

- Integrado en un tercer radio de banda doble específico (sin afectar el rendimiento del punto de acceso).

  Operbes S.A. de C.V. tomó en consideración que el servicio de Protección en Redes Inalámbricas se proveerá a través de un appliance de propósito específico.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 311 de la empresa Operbes, S.A. de C.V.

- Permitir aplicar políticas de control sobre las aplicaciones que los dispositivos

- Permitir la instalación de aplicaciones y ejecutar actualizaciones en múltiples dispositivos a la vez de manera remota y controlando el tipo de conexión y la fecha de ejecución
- Permitir realizar modificaciones de cambio de contraseña de bloqueo, y también se puede configurar la longitud, el tipo de contraseña, si es alfanumérica o numérica, el número de intentos, entre otros.

- Permitir a los administradores del sistema mantener y controlar estos dispositivos de forma centralizada.

- Analizar los dispositivos para asegurarse de que cumplen con la política del Instituto.

- Recuperar toda la información sobre los dispositivos, incluidos los detalles del dispositivo, certificados, aplicaciones instaladas, entre otros.

- Regular el acceso a las cuentas Institucionales tales como cuentas de correo electrónico, Wi-Fi y VPN.

- Bloquear los dispositivos de forma remota para evitar robados o perdida de información.

  Operbes S.A. de C.V. tomó en consideración que incluirá dentro de nuestra propuesta técnica una solución de MDM.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 675 de la empresa Totalsec, S.A. de C.V.

  Operbes S.A. de C.V. tomó en consideración queel servicio de protección de redes inalámbricas requiere un servicio tipo MDM para dar cumplimiento a lo establecido en el numeral 6.2.5 del anexo técnico de la Convocatorio.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 32 de la empresa Totalsec, S.A. de C.V.

- Soportará la conexión desde dispositivos móviles y de escritorio a través de un cliente de acceso remoto. Dicho cliente soportará al menos las siguientes plataformas operativas: MAC OS X, iOS, Android, Windows desde v7.

  Operbes S.A. de C.V. tomó en consideración que la versión Mac OS X 10.4.10 fue liberada en junio de 2007 y que el fabricante recomienda la actualización a Mac OS 10.13, el cliente de acceso remoto tendrá soporte para la versión 10.13 conforme a las recomendaciones en materia de seguridad.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 477 de la empresa Scitum, S.A. de C.V.

  Operbes S.A. de C.V. tomó en consideración que la versión la versión iOSv4 fue liberada en junio de 2010 y que el fabricante recomienda la actualización a iOS v6, el cliente de acceso remoto tendrá soporte para la versión 6 conforme a las recomendaciones en materia de seguridad.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 478 de la empresa Scitum, S.A. de C.V.

- Alarmas.

**6.2.6. Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA).**

**Descripción del Servicio.** Operbes S.A. de C.V. tomó en consideración que el Instituto requiere un servicio de control de acceso para usuarios privilegiados con la intención de entregar en los servidores las funcionalidades de control y monitoreo de las cuentas de usuarios privilegiados existentes en cada uno de ellos, así como un mecanismo de Autenticación, Autorización y Contabilización (AAA por sus siglas en inglés, Authentication, Authorization and Accounting), Operbes S.A. de C.V. cumplirá con las siguientes especificaciones funcionales mínimas.

Operbes S.A. de C.V. tomó en consideración que se acepta que derivado que llegan a existir contraseñas (SA, Admin, Root, etc), la solución a proponer por los participantes permita resguardar (bóveda digital) aquellas claves o contraseñas consideradas por el instituto como de misión crítica; donde la solución permita recuperar las credenciales y se puede acceder a ellas de manera remota.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 676 de la empresa Totalsec, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que se integrarán con este servicio será el autenticación para redes inalámbricas.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 678 de la empresa Totalsec, S.A. de C.V.

- Contar con una solución tecnológica que controle de manera granular el acceso a los activos de infraestructura que soportan las aplicaciones, a través de la administración del ciclo de vida de identidades.
- Integrar procesos que identifique los roles y perfiles de cada usuario por aplicación, así como la trazabilidad de los accesos realizados.
- Considerar, de manera enunciativa más no limitativa, las siguientes plataformas operativas:
  - Microsoft Windows
  - Unix
  - Linux
- Revisar y validar en conjunto con el Instituto los requerimientos de protección de las claves privilegiadas en los servidores en que se vaya a habilitar para el servicio.
- Implementar los agentes propiciados por la solución en sistemas operativos soportados por los fabricantes correspondientes.
- Operbes S.A. de C.V. llevará a cabo todas las tareas necesarias para la instalación del equipo en la zona de los Centro de Datos donde le sea solicitado.
- Operbes S.A. de C.V. acordará con el personal del Gobierno de Contrato las ventanas de mantenimiento necesarias según el tiempo de implementación del que se trate.
- Operbes S.A. de C.V. integrará el dispositivo hacia la consola de administración de la solución, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Servicios de autenticación, autorización y registro (AAA) para habilitar el control de acceso e identidad hacia la red del Instituto.
- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).
- Uso de RADIUS la autenticación de acceso a la red.
- Uso de TACACS+ para la autenticación para accesos administrativos a la infraestructura del Centro de Datos.
- Será capaz de soportar la administración de al menos 5,000 dispositivos de red.
- Administración centralizada para políticas de acceso de gestión y VPN.
- Capacidad de generar políticas basadas en reglas y atributos.
- Capacidad de generación de políticas con asignación de VLANs.
- Integración con bases de datos externas tales como Active Directory y LDAP.

- Capacidad de integrarse a un dominio de Directorio Activo.
- Integración con soluciones de contraseñar únicas.
- Integración con los dispositivos de red para asegurar la aplicación de políticas de seguridad basadas en identidad.
- Uso de los siguientes protocolos de autenticación:
  - CHAP/MSCHAP
  - PAP
  - PEAP
  - EAP-TLS
  - MS-CHAP
  - EAP-MD5

  Operbes S.A. de C.V. tomó en consideración que los siguientes protocolos de autenticación mencionados en
  este punto, corresponden al volumen de los 5 mil dispositivos.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 684 de la empresa Totalsec, S.A. de C.V.
- Generación de políticas de restricciones por dispositivo y hora del día.
- Uso de listas de acceso descargables.
- Capacidad de operar en esquemas conglomerados (clúster) con más de 3 dispositivos operando como un solo sistema.
- Capacidad de operar en esquemas de procesamiento físico (appliance) o virtualizados
- Interface de administración gráfica basada en web
- Interface de programación para actualizar, crear, leer y borrar operaciones de dispositivos, terminales y usuarios de la base de datos interna.
- Funciones de reporteo y auditoría
- Capacidades de monitoreo y diagnóstico de problemas
- Administración de mensajes de eventos (logs) exportables.

**6.2.7. Servicio de Antivirus**

**Descripción del servicio.** Operbes S.A. de C.V. proporcionará el licenciamiento, instalación, habilitación, configuración, puesta a punto, gestión, monitoreo, soporte y mantenimiento de una solución, que pueda poner en riesgo su funcionalidad, comprometiendo la seguridad en la actividad de los usuarios.

Operbes S.A. de C.V. tomó en consideración que el alcance del servicio no contempla laptops y/o desktops.
Operbes S.A. de C.V. tomó en consideración que en cuanto a los servidores, el inventario le será proporcionado al licitante adjudicado.
Operbes S.A. de C.V. tomó en consideración que respecto a los sistemas operativos se tienen contemplados al menos: Windows Server 2012, Windows Server 2016, Windows Server 2019 o mayor

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 54 de la empresa Axtel, S.A.B. de C.V.

La protección de antivirus se realizará a través de un agente, el cual será distribuido a los activos de infraestructura que el Instituto solicité, siendo responsabilidad de Operbes S.A. de C.V. garantizar la entrega de dicho agente a los activos de infraestructura indicados por el Instituto, la distribución y administración puede ejecutarse onpremise o nube.

Operbes S.A. de C.V. considerará que las actividades de remediación en infecciones de virus, serán su responsabilidad, por lo que brindará el apoyo correspondiente a través de la explotación de las funcionalidades de la solución del antivirus propuesta como parte del presente servicio. Operbes S.A. de C.V. notificará al personal que Instituto designe sobre los hallazgos de actividad sospechosa vía correo electrónico, u otro mecanismo que ambas partes determinen. Operbes S.A. de C.V. atenderá los incidentes de *malware* que puedan presentarse; conforme se determine en los Acuerdos de Nivel de Servicio, o en su caso, a los Acuerdos de Nivel Operativos.

Cuando la necesidad de instalación del Instituto sea de más de 200 agentes, Operbes S.A. de C.V. , en conjunto con el Instituto, definirán una estrategia que permita el despliegue del agente de Antivirus, así como adecuar la estrategia de entrega de actualizaciones de Antivirus en cada uno de los activos de infraestructura solicitados, sin afectar la operación del Instituto, considerando que dichos activos y consolas de administración se encontrarán distribuidos en las diferentes localidades del Instituto.

Operbes S.A. de C.V. configurará en la solución de Antivirus propuesta, las políticas base de seguridad definidas en conjunto con el Instituto, como parte de las reglas que regirá el presente servicio, para los activos de infraestructura a los cuales les sea provisto, la cual será desplegada a los mismos a través de la consola de administración de la solución. A su vez, Operbes S.A. de C.V. realizará la puesta a punto de las políticas definidas en la solución de antivirus propuesta, con fundamento en el monitoreo continuo de la misma y los requerimientos del Instituto.

Operbes S.A. de C.V. definirá una estrategia en conjunto con el Instituto que permita el despliegue para la entrega de actualizaciones de Antivirus en cada uno de los activos de infraestructura sin afectar las operaciones de los servicios internos, los cuales se encuentran distribuidos en las diferentes localidades de la CDMX. Será responsabilidad de Operbes S.A. de C.V. mantener actualizados en todo momento los activos de infraestructura con la última versión o actualización de antivirus liberada por el fabricante.

Operbes S.A. de C.V. , en conjunto con el Instituto, definirá la cantidad de activos de infraestructura que constituirá la línea base para el primer año de prestación del servicio. Posteriormente, un mes antes de cumplir cada año de servicio se realizará una redefinición de la línea base para la prestación del servicio del próximo año.

Operbes S.A. de C.V. entregará al personal del Instituto la última versión del agente de antivirus, para que este sea integrado dentro de la imagen de software de los Puestos de Servicio.

Como parte de la operación del presente servicio, Operbes S.A. de C.V. :

- Emitirá alertas de incidentes y monitoreará los eventos generados por los elementos tecnológicos de la solución de Antivirus.
- Monitoreará el cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificará sobre las actividades sospechosas relacionadas con la infección de activos de infraestructura.
- Notificará sobre todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la Solución de Antivirus, efectuando la contención de las mismas a través de la solución propuesta.

- Resolverá las solicitudes de soporte técnico especializado, a fin de evitar y prevenir infecciones en los activos de infraestructura donde se encuentre instalada la solución de Antivirus.
- Recolectará e integrará, al menos la información de eventos de seguridad o logs generada por la solución de Antivirus, hacia la solución de correlación de eventos, cuyo detalle de información a integrar será definido entre el Instituto y Operbes S.A. de C.V. .
- Desarrollará la afinación de la solución con base en el resultado del monitoreo continuo, además de gestionar las reglas antivirus en los activos de infraestructura, con base en las necesidades del Instituto y en el resultado del monitoreo día a día.

**6.2.8. Servicios de Prevención de Pérdida de Información**

**Descripción del servicio.** Operbes S.A. de C.V. tomó en consideración que el Instituto requiere una solución que permita detectar y evitar la fuga y/o pérdida de información sensible en los activos de infraestructura del IMSS instalados en los Centros de Datos, misma que estará integrada a los activos de infraestructura, servicio de correo electrónico externo, correo electrónico interno, navegación web y portales de colaboración, para una completa visualización y prevención en distintas capas de seguridad.

Operbes S.A. de C.V. tomó en consideración que el servicio de Prevención de Pérdida de Información se proveerá a través de appliances de propósito específico y a través de agentes que se instalen en servidores / PCs / Laptops, por lo tanto a través de ambas modalidades.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 315 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que al referir ambas modalidades puede ser a través de agentes y/o appliances de propósito especifico siempre y cuando se cumpla con las características solicitadas para el servicio.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 21 de la empresa Operbes, S.A. de C.V.

Dicho módulo tendrá la capacidad de generar políticas a través de palabras clave o expresiones regulares con la información sensible, bloqueando su transmisión a través de diversos canales de comunicación.

El servicio se enfocará en prevenir fuga de información sensible desde los puestos de servicio.

Operbes S.A. de C.V. configurará en la solución propuesta las políticas base de seguridad definidas en conjunto con el Instituto, para los activos de infraestructura, desarrollando los perfiles correspondientes.

Dichas políticas serán desplegadas a través de la consola de administración de la solución, y Operbes S.A. de C.V. realizará la puesta a punto de las mismas, con fundamento en su monitoreo continuo y los requerimientos del Instituto, para lo cual, el Instituto requiere que se tomen en consideración, como mínimo, las siguientes premisas:

- Tipos de documentos.
  Operbes S.A. de C.V. tomó en consideración que se refiere a las formas en las cuales se pueden estructurar los activos de información que son relevantes para los procesos del Instituto: reportes, estudios, oficios, correspondencia, acuerdos, directivas, planes estratégicos, contratos, convenios, anotaciones, memorandos, estadísticas, procedimientos, políticas, reglamentos, informes, solicitudes, encuestas, históricos, entre otros.

- Medios de almacenamiento de la información.

Operbes S.A. de C.V. tomó en consideración que se refiere a los distintos medios en los cuales pueden resguardarse los activos de información para su posterior manipulación

Operbes S.A. de C.V. asegurará que las funcionalidades de la Solución de Prevención de Pérdida de Información se cumplirán aun cuando el activo de infraestructura no se encuentre firmado a ningún Directorio Activo, o bien, a la red del Instituto.

Como parte de la operación del servicio, Operbes S.A. de C.V. :

- Emitirá alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Prevención de Pérdida de Información.
- Monitoreará el cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificará al Instituto sobre actividades sospechosas relacionadas con la violación de las políticas sobre fuga de información configuradas en los activos de infraestructura.
- Efectuará la contención de actividades sospechosas.
- Atenderá a las solicitudes de soporte técnico especializado, a fin de evitar fugas de información en los equipos en los que se encuentre habilitada la solución.
- Recolectará e integrará, al menos la información de eventos de seguridad o logs generada por la solución de Prevención de Pérdida de Información, hacia la solución de correlación de eventos, cuyo detalle de la información a integrar será definido entre el Instituto y el proveedor.
- Administrará los elementos tecnológicos a través de procesos de gestión de cambios, configuraciones y versiones de acuerdo con los requerimientos del Instituto.

La solución propuesta por Operbes S.A. de C.V. contará con las siguientes funcionalidades:

- Presente un log de auditoría de todas las actividades de los usuarios.
- Proporcione reportes predefinidos y personalizados que puedan ser programados o de una sola vez.
- Proporcione un mecanismo de alertas y notificaciones.
- Tecnología de Detección.
  - Capacidad para extraer textos de diferentes tipos de documentos para ejecutar escaneos de contenido.
  - Capacidad de realizar detecciones basadas en palabras (keywords) personalizadas o frases (key phrases) personalizadas, con la habilidad de poner diferentes palabras en una sola regla de detección.
- Será capaz de ejecutar escaneos de contenido en diversos canales de información (Correo, https/http, ftp, entre otros)

**6.2.9. Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)**

**Descripción del servicio.** Garantizar la continuidad operativa del Sistema de Gestión de Seguridad de la Información (SGSI), que estará basado en el estándar ISO/IEC 27001:2013, mediante el cual se emitirán las directivas en materia de seguridad de la información a las áreas de TI y a los terceros que soportan la operación de TI, mismo que considerará las actualizaciones que correspondan.

Operbes S.A. de C.V. garantizará la continuidad operativa de este servicio y cumplirá con al menos las siguientes funcionalidades operativas:

**Planear**

- Capacitación de seguimiento – Curso "Inducción a la norma ISO/IEC 27001:2013 o vigente, que permita:
  - Conocer la estructura de la norma ISO/IEC27001:2013

- Interpretar los requisitos solicitados para el cumplimiento de la norma
- Conocer las etapas para la implementación de un SGSI
- Se considerará al menos 8 participantes, con un tiempo mínimo de 8 horas y máximo de 40 horas.

Operbes S.A. de C.V. tomó en consideración que al menos serán dos sesiones y el formato se definirán en una mesa de trabajo con el licitante adjudicado.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 449 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que Los cursos de inducción se llevarán a cabo de manera presencial previo acuerdo entre el Licitante adjudicado y el Administrador del contrato.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 587 de la empresa Scitum, S.A. de C.V.

- Seguimiento y actualización en la aplicación de las directivas en materia de seguridad.
Manual de políticas de seguridad de la información, que se apegará a lo siguiente:
  - Dominios que establece la norma ISO/IEC 27001:2013
  - Procesos de seguridad aplicables en la normativa vigente.
  - Enfocarse a las áreas de TI y a los terceros que proveen servicios de TI al Instituto, considerando como alcance el catálogo de infraestructuras críticas del Instituto (al menos 20 directivas).

- Identificación y evaluación de activos (relacionado al catálogo de infraestructuras críticas) del proceso involucrado en el Sistema de Gestión de Seguridad de la Información.
La metodología considerará los siguientes temas:
  - Identificación de los activos del proceso.
  - Valoración de los activos del proceso.
  - Identificación de requerimientos de seguridad.
  - Identificación de los controles de seguridad existentes.

- Generación de la declaración de aplicabilidad. (SoA: Statement of Applicability).

  La metodología considerará los siguientes temas:
  - Identificación y aplicabilidad de los requerimientos internos y externos
  - Selección de los objetivos de control y controles para el tratamiento de los riesgos
  - Verificación de requerimientos contractuales y legales
  - Identificación de los requerimientos internos y externos
  - Validación de aplicabilidad de los requerimientos
  - Formato de Autorización para implantar y operar el Sistema de Gestión de Seguridad de la Información
  - Preparación de la declaración de aplicabilidad
  - Documentar los objetivos de control y los controles elegidos y la justificación de su elección
  - Documentar los controles actualmente implementados
  - Documentar la exclusión de controles y la justificación de su exclusión

- Operación el Sistema de Gestión de Seguridad de la Información
  - Análisis de Riesgos de Seguridad de la Información
  - Análisis de riesgo con base en lo definido en el servicio de gestión de riesgos de seguridad
    Operbes S.A. de C.V. tomó en consideración que el servicio de gestión de riesgos de seguridad será provisto por el Instituto.
    Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 451 de la empresa Scitum, S.A. de C.V.

- Generación de la actualización del plan de tratamiento de riesgos
  La metodología considerará los siguientes temas:
  - Identificación de las acciones a realizar por parte de la institución y su administración
  - Identificación de los recursos necesarios y prioridades
  - Identificación de las responsabilidades para administrar los riesgos de seguridad de la información

- Aplicación del seguimiento al plan de tratamiento de riesgos.
  La metodología considerará los siguientes temas:
  - Asignación de los roles y responsabilidades en el seguimiento de los controles relativos a personas, procesos y tecnología involucrados en la mitigación de los riesgos.
  - Actualización de documentación, alineada a los requisitos establecidos en la normativa vigente

- Detalle y actualización de políticas y procedimientos de seguridad existentes

- Definición del proceso de reporte y atención de incidentes de seguridad

- Propuestas de implementación de los controles seleccionados.
  La metodología considerará los siguientes temas:
  - Control de accesos
  - Monitoreo de cuentas
  - Definición del proceso de Continuidad del negocio
  - Implantación de los Roles y responsabilidades definidas para el Sistema de Gestión de Seguridad de la Información
  - Controles de seguridad en la infraestructura tecnológica de acuerdo con lo definido en el alcance.

- Administración del cambio cultural.
  La metodología considerará los siguientes temas:
  - Actualización del Programa de concientización con usuarios y operadores del Sistema de Gestión de Seguridad de la Información
  - Seguimiento y apoyo a las necesidades de capacitación para el personal que administra el Sistema de Gestión de Seguridad de la Información y seguridad de la información
  - Manual de Gestión de Seguridad de la Información.
    Se documentará un manual que contenga las referencias generadas en esta fase para dar trazabilidad al de las cláusulas de la norma.

  Operbes S.A. de C.V. tomó en consideración que el número de usuarios y operadores del del Sistema de Gestión
  de Seguridad de la Información incluidos en el programa de concientización al menos 8 participantes, de acuerdo con lo establecido en el numeral 6.2.9. Servicios de Sistema de Gestión de Seguridad de la Información (SGSI) del anexo técnico.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 592 de la empresa Scitum, S.A. de C.V.

- Monitorear y Revisar el Sistema de Gestión de Seguridad de la Información
  Revisiones gerenciales.
  La metodología considerará los siguientes temas:
  - Los dueños del proceso harán una revisión y actualización al Sistema de Gestión de Seguridad de la Información con la finalidad de verificar que los objetivos del Sistema de

Gestión de Seguridad de la Información están alineados a los objetivos de negocio en materia de seguridad de la información y que garantizan el adecuado manejo de los riesgos existentes.
- Operbes S.A. de C.V. actualizará el procedimiento de revisiones gerenciales.
- Operbes S.A. de C.V. actualizará los formatos requeridos para llevar a cabo las revisiones gerenciales

- Auditorías internas.
  La metodología considerará lo siguiente:
  - Seguimiento y apoyo en la generación del plan de auditorías internas a las áreas de TI y a los terceros que proveen servicios de TI al Instituto.
  - Actualización o en su caso definición de los formatos requeridos para llevar a cabo las auditorías
  - Aplicación de una auditoría interna al Sistema de Gestión de Seguridad de la Información para verificar el cumplimiento con el estándar ISO/IEC 27001:2013 o vigente y a los procesos establecidos en la normativa vigente aplicable.

  Operbes S.A. de C.V. tomó en consideración que las auditoras internas serán en la Ciudad de México y será proporcionado en una mesa de trabajo al licitante adjudicado la duración máxima de la auditoria.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, preguntas 593 y 594 de la empresa Scitum, S.A. de C.V.

- Actualización del Sistema de Gestión de Seguridad de la Información
  Implementación de mejoras
  Considerará los siguientes temas:
  - Priorización de las acciones correctivas y no conformidades identificadas en las revisiones gerenciales, revisiones independientes, auditorías internas y revisiones técnicas
  - Identificación de los responsables de llevar a cabo las mejoras.
  - El Instituto definirá las fechas compromiso para la terminación de las mejoras, únicamente para seguimiento interno.

- Acciones correctivas y no conformidades.
  Considerará lo siguiente:
  - Apoyo en la definición y seguimiento del procedimiento para realizar acciones correctivas y no conformidades derivadas de las auditorias.
  - Actualización del formato para llenado de acciones correctivas y no conformidades.
  - Coordinación de la ejecución de las acciones correctivas ya definidas y en su caso las no conformidades que se identifiquen.

- Comunicar los resultados de las acciones tomadas.
  Se considerará lo siguiente:
  - Apoyo en la programación de reuniones de seguimiento al Sistema de Gestión de Seguridad de la Información para dar a conocer el alcance de las acciones correctivas y no conformidades realizadas y verificar su apego a los requerimientos de los dueños de la información y a los involucrados en los procesos del Instituto.

**6.2.10. Servicios Continuidad de Gestión del Cambio en Seguridad de la Información**

**Descripción del servicio.** Operbes S.A. de C.V. tomó en consideración que el Instituto requiere de la integración de un programa de gestión del cambio para la protección de la información, alineado a los requerimientos del estándar ISO/IEC27001:2013, siguiendo una estrategia cultural.

Este servicio contará con un plan de transferencia de conocimiento al personal del Instituto en los principales temas de seguridad de la información considerando al menos los siguientes rubros:

- Regulación vigente en materia de seguridad de la información.
- Políticas de seguridad del Instituto.
- Procesos de seguridad del Instituto.
- Controles de seguridad implementados en el Instituto.
  Operbes S.A. de C.V. tomó en consideración que la cantidad de áreas en los que aplican los servicios de continuidad de Gestión del cambio en seguridad de la información es una dirección Normativa. En la cual se aplican al menos 18 políticas los Servicios Continuidad de Gestión del Cambio en Seguridad de la Información. Aplica un proceso de seguridad de la información y al menos 18 controles de seguridad.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 586 de la empresa Scitum, S.A. de C.V.
  Operbes S.A. de C.V. tomó en consideración que el número de personal que se aplicará el plan de transferencia será de al 40 usuarios
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 595 de la empresa Scitum, S.A. de C.V.

El servicio se describe en las etapas que a continuación se indican:

Etapa 1. Definición de la estrategia de gestión del cambio

- Contextualización del Instituto. Operbes S.A. de C.V. tendrá el contexto cultural del Instituto en materia de seguridad de la información
- Diagnóstico del estado actual. Operbes S.A. de C.V. llevará a cabo un diagnóstico del nivel de conocimiento en materia de seguridad de la información que presente la brecha entre la situación actual y la situación requerida por el Instituto
- Preparación de la estrategia. Operbes S.A. de C.V. , con base en los resultados obtenidos en el diagnóstico, propondrá una estrategia de gestión del cambio en seguridad de la información con el fin de hacer una adecuada transferencia del conocimiento.
  Operbes S.A. de C.V. tomó en consideración que el número de personal que se llevará acabo el diagnostico será máximo 300 usuarios.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 596 de la empresa Scitum, S.A. de C.V

Etapa 2. Diseño del programa de gestión del cambio

- Preparación del programa. Operbes S.A. de C.V. generará un plan de trabajo detallado con los temas que forman parte de la transferencia del conocimiento, el número de personal involucrado y las fechas en las cuales se llevará a cabo.
- Preparación de contenidos. Operbes S.A. de C.V. desarrollará los materiales en formato Power Point, u otros que el Instituto defina, que serán utilizados para la transferencia del conocimiento en seguridad de la información.
- Generación del modelo de evaluación. Operbes S.A. de C.V. presentará un modelo de evaluación con el fin de identificar el grado de efectividad de la transferencia de conocimiento de seguridad de la información.

- Preparación del grupo de train traineers. Operbes S.A. de C.V. identificará y preparará a un grupo de 5 trainees con el fin de que puedan replicar la transferencia del conocimiento a otras áreas sustantivas dentro del Instituto.

  Operbes S.A. de C.V. tomó en consideración que el número máximo de horas disponibles para identificar y preparar a un grupo de 5 trainees con el fin de que puedan replicar la transferencia del conocimiento a otras áreas sustantivas dentro del Instituto será máximo 40 usuarios.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 597 de la empresa Scitum, S.A. de C.V.

Etapa 3. Comunicación del programa de gestión del cambio

- Despliegue de la transferencia. Operbes S.A. de C.V. llevará a cabo el despliegue de la transferencia del conocimiento al personal de TI del Instituto y de las áreas sustantivas definidas por este dentro de la Ciudad de México.

  Operbes S.A. de C.V. tomó en consideración que el número de personal para esta etapa será de al menos 40 usuarios.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 598 de la empresa Scitum, S.A. de C.V

  Operbes S.A. de C.V. tomó en consideración que el número de áreas sustantivas definidas por el Instituto será un dirección normativa.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 599 de la empresa Scitum, S.A. de C.V

Etapa 4. Medición del programa de gestión del cambio

- Aplicación de evaluaciones. Operbes S.A. de C.V. habilitará una herramienta tecnológica con el fin de aplicar evaluaciones en línea a los participantes de la transferencia del conocimiento.
- Análisis de datos obtenidos. Operbes S.A. de C.V. revisará la información obtenida con el fin de organizar los resultados obtenidos.
- Presentación de resultados generales. Operbes S.A. de C.V. llevará a cabo una presentación ejecutiva con los resultados obtenidos al personal de TI del Instituto.

## 6.3. Servicios del Centro de Operaciones de Seguridad (SOC)

Operbes S.A. de C.V. cuenta con un Centro de Operaciones de Seguridad (SOC), que se encuentre físicamente en las instalaciones de Bestel. El objetivo de este centro será la continuidad operativa a la gestión de la seguridad, así como el responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad, que ejecute actividades de revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, así como el establecimiento de acciones de mejora sustentable.

El servicio del Security Operatión Center (SOC) que soportará la operación y prestación del servicio requerido por el Instituto, proporcionará un control continuo, una mayor eficiencia y oportunidad de mejora, para lo anterior Operbes S.A. de C.V. proporcionará servicios de tecnología de la información fiables en lo referente a la gestión de servicios de TI, mismos que acredita con las certificaciones ISO/IEC27001:2013 e ISO/IEC 20000-1:2018 vigentes y a nombre de Operbes S.A. de C.V. Para dar cumplimiento con este punto

favor de referirse al documento llamado "certificados ISO/IEC27001:2013 e ISO/IEC20000-1:2018 vigentes" dentro de la presente propuesta técnica.

Operbes S.A. de C.V. tomó en consideración que se acepta que para dar un servicio de SOC con mejor calidad y que tenga la capacidad de establecer y llevar a cabo un plan de continuidad apegado a la operación de la convocante, es necesario que el SOC de Operbes S.A. de C.V. este certificado no sólo en ISO/IEC27001:2013 e ISO/IEC20000-1:2018, sino también en ISO/IEC 22301:2019 e ISO/IEC 9001:2015
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 338 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. considera que el servicio de SOC se refiere a las soluciones propuestas e implementadas hoy en día por el instituto, así mismo considera que la correlación de bitácoras se basará en un servicio de correlación de eventos e incidentes de seguridad en el que los casos de uso serán ilimitados, así como las respuestas ante un incidente alineadas a tiempo de los niveles de servicio (SLA) establecidos para este servicio.

- Se ubica dentro de territorio nacional, mismo que acredita con la copia simple a nombre del SOC de Operbes S.A. de C.V. del ISO/IEC27001:2013 e ISO/IEC20000-1:2018. Para dar cumplimiento con este punto favor de referirse al documento llamado "certificados ISO/IEC27001:2013 e ISO/IEC20000-1:2018 vigentes" dentro de la presente propuesta técnica.

- Operación continua las 24 horas del día, los 7 días de la semana y durante los 365 días del año (7x24x365), esto último conforme la vigencia del contrato.

- Cuenta con personal para la atención del servicio en sitio y de forma remota, el cual es personal calificado con base en las credenciales requeridas para la administración y monitoreo de los componentes que integran la solución.

- Operación en un centro de datos alterno ubicado dentro de territorio nacional.

- Mantenimiento de las suscripciones a sitios y listas de empresas, fabricantes y medios especializados en seguridad de la información, que permitan alertar sobre nuevas vulnerabilidades.

- Infraestructura dedicada para la administración, operación y monitoreo de los componentes *hardware* y *software* que componen los servicios de seguridad.

- Realizará evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones se ejecutarán cada 3 meses, desde el inicio de operaciones de los servicios y hasta 3 meses antes del término de estos.

- Realizará acciones correctivas y preventivas para asegurar la confidencialidad, integridad y disponibilidad de la información que se maneja en las diferentes soluciones se seguridad.

- Notificaciones y alertas personalizadas, en caso de desviaciones, anormalidades o brechas de seguridad, para cada una de las soluciones de seguridad.

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

- Analiza los eventos de seguridad y administración de bitácoras que se integran en los servicios de correlación de información, a fin de establecer acciones preventivas a través de modificaciones a las configuraciones de las soluciones de seguridad.

- Integra un Equipo de Atención y Respuesta a Incidentes de Seguridad.

- Soportará y dará Atención a fallas a los componentes hardware y software que integran la solución, conforme los estipulado en los acuerdos de niveles de servicio.
- Monitoreará la disponibilidad de los componentes hardware y software que integran la solución ofertada. La solución de monitoreo tendrá la capacidad de generar alertas y notificaciones en caso de fallas, degradación del desempeño de procesamiento de información, intermitencia y/o pérdida de disponibilidad.

- Realizará mantenimiento preventivo y correctivo a las soluciones de seguridad habilitadas, así como a los activos de infraestructura que soportan cada servicio.

- Ejecutará procesos operativos para al menos los siguientes rubros:

  - Gestión de Riesgos
  - Gestión de Continuidad
  - Monitoreo y Detección
  - Gestión de Seguridad de la información
  - Administración de Dispositivos
  - Gestión de solicitudes de servicio
  - Administración de Cambios Operacionales
  - Administración de Configuraciones
  - Administración de Vulnerabilidades
  - Gestión de Incidentes
  - Gestión de Problemas

  Operbes S.A. de C.V. tomó en consideración que los procesos referidos corresponden a la partida 1. Las certificaciones ISO27001 e ISO20000 vigentes se presentará para la partida 1 y 2.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 191 de la empresa All Service In Telecom and Medice S. de R.L. de C.V.

- Integración de una Mesa de servicio apegada a ITIL v4, la cual se integrará con la Mesa de Servicios Tecnológicos del Instituto, considerando todas las actividades de puesta a punto, desarrollo de piezas de software, configuraciones, entre otros, que permitan establecer la comunicación para la generación de requerimientos, cambios, incidentes, y otros procesos que determine el Instituto.

  Operbes S.A. de C.V. tomó en consideración que el alcance de la integración Consiste principalmente en la atención de requerimientos relacionados con los servicios que se pretenden contratar. El sistema que amplia actualmente es BMC-Remedy. La integración de la mesa estará compuesta por comunicación, personal especializado, herramientas a nivel técnico, procesos y de niveles de servicio del proveedor adjudicado y el Instituto. Operbes S.A. de C.V. tomó en consideración que se definirá en una mesa de trabajo con el licitante adjudicado.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 455 de la empresa Scitum, S.A. de C.V.

- El servicio de requerimientos, cambios, incidentes, entre otros, permitirá la generación de eventos (tickets), mediante los mecanismos que se establezcan en las mesas de trabajo correspondiente, que, de manera enunciativa más no limitativa, podrán ser:
  - Un número telefónico directo en las instalaciones del SOC.

- Un número telefónico a diez dígitos.
- Correo Electrónico
- Portal Web

- El personal de Operbes S.A. de C.V. , que atenderá las operaciones de los servicios de seguridad, contará con experiencia probada en las áreas de tecnología y de seguridad de la información previamente mencionadas, para lo cual, se integrará el currículo vitae de todo el personal que participe en el servicio, indicando al menos:
  - Experiencia profesional: bajo este rubro, se considerarán todos los puestos que cada integrante haya desempeñado, con fecha, nombre de los empleadores, nombre de los puestos que ha ejercido y el tipo de funciones bajo su responsabilidad, y contará con experiencia comprobable al menos 3 años.

  - Experiencia en proyectos de su especialidad en Seguridad de la Información: bajo este rubro se citarán y describirán todos los proyectos en que se ha participado, y contará con experiencia comprobable de al menos 3 años.

  - Estudios: bajo este rubro se anotarán todos los estudios en materia de seguridad de la información, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica. Las certificaciones son de tecnología y/o de seguridad de tipo "vendor-neutral".

    Operbes S.A. de C.V. tomó en consideración que se proporcionaran las certificaciones establecidas en el numeral 6.8 perfil del proveedor de las bases de la licitación, misma que refieren a las habilidades y especialidades de cada recurso requerido por el instituto, con la finalidad de acreditar la experiencia para la prestación de los servicios.
    Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 193 de la empresa All Service In Telecom and Medice S. de R.L. de C.V.

  - Incluirá la estructura del grupo de trabajo, indicando por cada perfil las responsabilidades y competencias

- El Instituto podrá solicitar la revisión de la infraestructura de seguridad por un tercero en cualquier momento, durante la vigencia del contrato, con la finalidad de dar certeza de la entrega del servicio.

- Seguimiento a la Base de Datos de la Gestión de la Configuración (CMDB por sus siglas en ingles) que contenga los detalles relevantes de cada elemento de configuración (CI) y de la relación entre ellos, incluyendo el equipo físico, software y la relación entre incidencias, problemas, cambios y otros datos del servicio de seguridad.

- Generará los reportes de Inteligencia de Negocio y Analítica de Información que permitan tener estadísticas del uso y desempeño de los servicios de seguridad, esto último con el objetivo de coadyuvar a la toma de decisión estratégica y operativa de los servicios, así como para determinar el plan de capacidad de cada tecnología implementada. Dichos reportes podrán considerar, de manera enunciativa más no limitativa, la siguiente información:

  - Estadísticas de uso de procesamiento por tecnología
  - Estadísticas de desempeño por tecnología (throughput)
  - Estadísticas de ataques informáticos bloqueados.
  - Estadísticas de comportamientos tipo esperado de uso por tecnología (líneas base)
  - Estadísticas de usuarios concurrentes por servicio.
  - Estadísticas de crecimiento diario, mensual y anual por cada servicio.

- Proporcionará al Instituto cuentas de acceso a las consolas de administración de los servicios de seguridad, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

  Operbes S.A. de C.V. tomó en consideración que las consolas de administración a las que hace referencia son las que pertenecen a la partida 1 y no a la partida 2
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 194 de la empresa All Service In Telecom and Medice S. de R.L. de C.V.

- Las consolas de administración provistas para los servicios de seguridad permitirán visualizar al menos:

  - Políticas: Control de Acceso
  - Configuraciones: Listas de Control de Acceso (Listas Blancas, Listas negras), Líneas base de seguridad.
  - Objetos: Usuarios, Grupos, Direcciones IP
  - Bitácoras.
  - Estadísticas en tiempo real: Desempeño, procesamiento, usuarios conectados, conexiones por segundo, ancho de banda utilizado.

  Operbes S.A. de C.V. tomó en consideración que las consolas de administración a las que hace referencia son las que pertenecen a la partida 1 y no a la partida 2
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 195 de la empresa All Service In Telecom and Medice S. de R.L. de C.V.

- Proporcionará al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para cada solución o servicio, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso de los servicios de seguridad.

- Integrará un Tablero de Estadísticas de Servicios de Seguridad a través de un portal único de administración de los servicios de seguridad de forma independiente a las consolas de administración de los servicios de seguridad, así como de las herramientas de monitoreo que contenga información estratégicas sobre el uso de los servicios en tiempo real y de manera histórica, y que permita al Instituto tener el contexto general sobre el desempeño de las soluciones, su estado de salud, incidentes registrados, reportes de actividades sospechosas relevantes a nivel mundial, u otra información relevante que permita tomar decisiones sobre las condiciones de operación de los servicios, Operbes S.A. de C.V. en caso de ser el licitante ganador incluye en su oferta económica los costos asociados al desarrollo para el cumplimiento de éste requerimiento.
  Operbes S.A. de C.V. tomó en consideración que integra un Tablero de Estadísticas de Servicios de Seguridad a través de un portal único de administración de los servicios de seguridad de forma independiente a las consolas de administración de los servicios de seguridad, así como de las herramientas de monitoreo que contenga información estratégicas sobre el uso de los servicios en tiempo real y de manera histórica, y que permita al Instituto tener el contexto general sobre el desempeño de las soluciones, su estado de salud, incidentes registrados, reportes de actividades sospechosas relevantes a nivel mundial, u otra información relevante que permita tomar decisiones sobre las condiciones de operación de los servicios.

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 69 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que el tablero de estadísticas de Servicios de Seguridad a través de un portal único a las que hace referencia son las que pertenecen a la partida 1 y no a la partida 2.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 196 de la empresa All Service In Telecom and Medice S. de R.L. de C.V.

- Permitirá al personal que designe el administrador del contrato, generar reportes explotando todas las variables y funcionalidades de la herramienta de monitoreo, con la opción de parametrizar dichos reportes y consultarlos vía web.

**6.5. Condiciones para la implementación de los servicios**

Operbes S.A. de C.V. en caso de ser el proveedor del servicio de SASI 2022-2024, será responsable de llevar a cabo la implementación de los servicios solicitados conforme a los plazos descritos en el presente documento, lo cual incluye las renovaciones o migraciones de tecnología que el cumplimiento de SASI 2022-2024, implique para la prestación puntual de dichos servicios.

Operbes S.A. de C.V. tomó en consideración que en todos los casos, los servicios se aceptarán siempre y cuando la totalidad de los componentes habilitadores, y sus funcionalidades requeridas, hayan sido correctamente entregadas y aceptadas por el Administrador del Contrato y las áreas del Instituto que se involucran, dependiendo de la naturaleza del servicio.

Operbes S.A. de C.V. en caso de ser el proveedor del servicio de SASI 2022-2024, considerará que el Instituto proveerá los servicios de energía eléctrica y hosting en los centros de datos y localidades donde residirán los componentes habilitadores requeridos para soportar cada uno de los servicios de SASI 2022-2024. Los insumos necesarios para la instalación, energización y todos los componentes de *hardware* y *software* necesarios para la incorporación de las soluciones propuestas por Operbes S.A. de C.V. en caso de ser el licitante ganador a la red del Instituto, será a cargo de Operbes S.A. de C.V. en caso de ser el licitante adjudicado.

Para la instalación, configuración y habilitación de cada una de las soluciones de los servicios, Operbes S.A. de C.V. en caso de ser el proveedor de SASI 2022-2024, considerará el apego a los procesos y procedimientos de control de cambios del Instituto para la integración de la infraestructura los Centros de Datos del Instituto. El detalle de estos procesos y procedimientos se proporcionarán en las Mesas de Trabajo entre Operbes S.A. de C.V. en caso de ser el licitante ganador de SASI 2022-2024, y el Instituto.

Es importante señalar que, Operbes S.A. de C.V. en caso de ser el licitante adjudicado contará con un proceso para la gestión de solicitudes que impliquen cualquier tipo de modificación o cambio en los componentes habilitadores requeridos en la descripción particular de cada uno de los servicios; para tal efecto, Operbes S.A. de C.V. en caso de ser el licitante ganador entenderá el control de cambios como la función de agregar, remover o modificar debidamente los componentes habilitadores y/o las configuraciones que lo necesiten, con la finalidad de ejecutar algún cambio orientado a satisfacer las necesidades del Instituto, sin afectar la continuidad de la operación, del negocio o de la seguridad de la información.

Operbes S.A. de C.V. tomó en consideración que el proceso de gestión de solicitudes de cualquier tipo de modificación o cambio estos serán registrados en el sistema de mesa de servicios alineado a ITIL v4 y el licitante adjudicado considerará lo necesario para que las solicitudes queden registradas y almacenadas en el sistema de mesa de ayuda.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 198 de la empresa All Service In Telecom and Medice S. de R.L. de C.V.

### 6.6. Implementación de los servicios

Las obligaciones contractuales mínimas de Operbes S.A. de C.V. en caso de ser el proveedor adjudicado, sin menoscabo de realizar aquellas que no estén incluidas en este apartado y que sean necesarias para cumplir con los requerimientos de servicio de SASI 2022-2024, son las siguientes:

- **Implementación de Servicios**: corresponde a la provisión, entrega, montaje e instalación física y lógica de todos los componentes de hardware, software, así como y puesta en marcha de todas las funcionalidades requeridas para cada uno de los servicios. Esto incluye conexiones a la red eléctrica e integración a la Red, así como asegurar la interoperabilidad con el resto de los componentes del Centro o los Centro de Datos del Instituto y ejecución de pruebas a nivel red y aplicativo, los componentes, equipos, accesorios, herramientas y todo lo necesario para el cumplimiento del presente apartado, queda incluido en la presente propuesta de Operbes S.A. de C.V. en caso de ser el licitante ganador.

  Operbes S.A. de C.V. tomó en consideración que implementación se definirá en una mesa de trabajo entre el Licitante adjudicado y el administrador del contrato.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 71 de la empresa Axtel, S.A.B. de C.V.

- **Migración de servicios Seguridad**: Corresponde a la responsabilidad de entregar un plan de migración, así como las correspondientes actividades en las que involucra migración de flujos de seguridad que se brindará en los componentes habilitadores que el proveedor de SASI 2022-2024, proveerá al Instituto. Estas actividades involucra a las tecnologías de conmutación, enrutamiento, centro de datos, seguridad, sin menoscabo de migrar aquellos flujos que no estén incluidas en este apartado y que sean necesarias para la entrega correcta del plan de migración requeridas en este proyecto, siendo los proveedores salientes quienes entreguen los flujos de comunicación y seguridad necesarios a Operbes S.A. de C.V. en caso de ser el proveedor de SASI 2022-2024, en forma documental al gobierno de contrato y áreas de tecnología involucradas del Instituto antes de comenzar las labores de implantación para su validación.

  Operbes S.A. de C.V. tomó en consideración que el instituto definirá en una mesa de trabajo aquellos servicios que
  serán migrados, asumiendo que, al inicio del servicio, Operbes S.A. de C.V. en caso de ser el Licitante adjudicado, dará continuidad operativa a los activos de infraestructura dispuestos en el Apéndice B.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 73 de la empresa Axtel, S.A.B. de C.V.

- **Operación estable del proyecto**: Pruebas integrales de todas las funcionalidades de los Componentes Habilitadores y la conectividad e interoperabilidad con el resto de los Componentes del Centro de Datos. Operbes S.A. de C.V. en caso de ser el proveedor adjudicado llevará a cabo la integración y pruebas de la infraestructura de Comunicaciones, Seguridad, *software* y de las herramientas asociadas que aseguren que toda la infraestructura y componentes que conforman, se encuentren operando correctamente como un solo sistema integral (pruebas de conectividad, reglas de flujos de comunicaciones, políticas de seguridad, funcionalidades, seguridad, monitoreo y gestión).

### 6.7. Mesas de Trabajo

Operbes S.A. de C.V. en caso de ser el proveedor adjudicado será responsable de integrar al servicio de SASI 2022-2024, una mesa de trabajo para la atención de los diferentes requerimientos que puedan surgir durante la vigencia del contrato.

Este servicio estará disponible a lo largo de la vigencia del presente contrato. De este modo, Operbes S.A. de C.V. en caso de ser el licitante adjudicado será el responsable de asignar personal con experiencia y expertos para conformar las mesa de trabajo. En caso de que el personal asignado sea retirado del servicio de SASI 2022-2024, será responsabilidad de Operbes S.A. de C.V. en caso de ser el licitante adjudicado notificar al Instituto con anticipación el motivo y fecha de su remoción de manera oficial. Así también será responsable de notificar de qué manera se llevará a cabo la sustitución del recurso en un esquema que garantice siempre la continuidad y calidad de los servicios requeridos.

Operbes S.A. de C.V. en caso de ser el proveedor adjudicado será responsable de instrumentar las mesas de trabajo tanto para las funcionalidades que utilice la infraestructura, así como también aquellas que impliquen una reingeniería de la misma, en las que se desarrollarán reportes de evaluación de postura de redes y seguridad del servicio, se documentarán conclusiones y recomendaciones de modificación de la infraestructura de la red y seguridad como mejora u optimización de la disponibilidad, capacidad y desempeño de los recursos y seguridad de las aplicaciones que vivan en los centros de datos del Instituto.

El Instituto podrá en cualquier momento de la vigencia del contrato de SASI 2022-2024, solicitar a Operbes S.A. de C.V. en caso de ser el proveedor adjudicado del servicio de diseño para cambios relevantes que se planeen efectuar en la infraestructura de red y seguridad que conforman el presente proyecto.

A continuación, se enlistan las responsabilidades mínimas que tendrá que llevar a cabo Operbes S.A. de C.V. en caso de ser el licitante adjudicado, sin menoscabo de realizar aquellas que no estén incluidas en este apartado y que sean necesarias para cumplir con los requerimientos solicitados.

- Generar reportes de estado de salud y proponer mejoras y/o soluciones arquitectónicas de la infraestructura de red y seguridad.
- Análisis de impacto de nuevos requerimientos que requieran el uso de la Infraestructura de red y seguridad existente en el contrato de SASI 2022-2024.
- Desarrollo de recomendaciones de optimización de anchos de banda, mejores rutas, optimización de la infraestructura.
- Diseño de mejoras sobre la infraestructura y recomendaciones que brinden el más alto desempeño y nivel de servicio.
- Entrega de reportes proactivos de recomendaciones de actualizaciones de software de los componentes habilitadores que conforman el contrato SASI 2022-2024.
- Entrega de reporte de análisis detallado del comportamiento de la red de comunicaciones y elementos de seguridad que conforman el contrato SASI 2022-2024.
- Todas las propuestas de configuración avanzada o configuración de nuevas funcionalidades propuestas por Operbes S.A. de C.V. en caso de ser el licitante ganador de SASI 2022-2024 estarán validadas por personal certificado y con experiencia de Operbes S.A. de C.V. en caso de ser el proveedor del servicio de SASI 2022-2024.
- Consultoría y recomendaciones de arquitectura de Centro de Datos en base a sus mejores prácticas, dimensionamiento, uso adecuado de recursos.
- Revisión de los requerimientos de diseño, prioridades y objetivos de acuerdo a lo especificado por el administrador del contrato.
- Revisión de la arquitectura y topología de la infraestructura de la red.
- Revisión de la configuración de protocolos.
- Revisión de la configuración de características de los servicios.
- Revisión de las mejores prácticas en materia de seguridad informática.
- Recomendación y diseños que permitan incrementar de manera notable las funcionalidades y que conforman la infraestructura tecnológica del Instituto.

**6.8. Perfil del Proveedor**

Operbes S.A. de C.V. contará con la capacidad, flexibilidad, solvencia económica y competencia técnica certificada que permita implementar y operar las soluciones de seguridad y sus mecanismos con todo lo necesario para su correcto funcionamiento, en los sitios en donde "EL INSTITUTO" lo requiera conforme a las características y especificaciones mencionadas en la presente propuesta Técnica.

El personal de Bestel, que atenderá las operaciones de los servicios de seguridad, contará con experiencia probada en las áreas de tecnología y de seguridad de la información previamente mencionadas, para lo cual, se integrará el currículo vitae de todo el personal que participe en el servicio, indicando al menos:

- Experiencia profesional: bajo este rubro, se considerarán todos los puestos que cada integrante haya desempeñado, con fecha, nombre de los empleadores, nombre de los puestos que ha ejercido y el tipo de funciones bajo su responsabilidad, y deberá contar con experiencia comprobable al menos 3 años.
- Experiencia en proyectos de su especialidad en Seguridad de la Información: bajo este rubro se citarán y describirán todos los proyectos en que se ha participado, y contará con experiencia comprobable de al menos 3 años.
- Estudios: bajo este rubro se anotarán todos los estudios en materia de seguridad de la información, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica. Las certificaciones son de tecnología y/o de seguridad de tipo "vendor-neutral".
- Incluirá la estructura del grupo de trabajo, indicando por cada perfil las responsabilidades y competencias.

Operbes S.A. de C.V. tomó en consideración que el currículo vitae de todo el personal que participe en el servicio, se acreditara siempre y cuando contenga todas y cada una de las características requeridas, por lo que el incumplimiento de la presentación de este, afectaría la solvencia de la propuesta.

Operbes S.A. de C.V. tomó en consideración que se acreditará al menos la licenciatura o ingeniería en informática, telecomunicaciones, computación o carrera a fin, en los términos que establece la Ley Reglamentaria del Art. 5 Constitucional, la acreditación será con el título y cédula profesional y para el caso de estudios en el extranjero, estos estarán avalados por las instancias oficiales correspondientes, así como estar debidamente apostillados.

Operbes S.A. de C.V. tomó en consideración que para acreditar el nivel académico del personal, Operbes S.A. de C.V. podrá presentar copia simple de la cedula y/o Título profesional de Licenciatura o Ingeniería en las áreas a fines a tecnologías de la Información y comunicación o áreas como sistemas, informática, computación, comunicación y electrónica, siempre y cuando sea verificable
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 109 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que un recurso puede cumplir uno más perfiles para la partida uno y partida dos, siempre y cuando se cumpla con la certificación requerida y la misma aplique.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 110 de la empresa Axtel, S.A.B. de C.V.

A continuación, se listan las credenciales y capacidades que cubrirá los recursos asignados al proyecto:

Operbes S.A. de C.V. tomó en consideración que no es necesario el personal en sitio, sim embargo, en el caso de ser necesario o de requerirse se tendrán que presentar en las instalaciones del Instituto.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 463 de la empresa Scitum, S.A. de C.V.

**Partida 1**

| Perfil | Certificaciones a demostrar | Experiencia a demostrar | Función | Numero de recursos |
|---|---|---|---|---|
| Administrador del Centro de Operaciones de Seguridad (SOC)<br><br>Operbes S.A. de C.V. tomó en consideración que el lugar de la prestación de servicio para este recurso y su esquema de atención ( remoto en el SOC de Bestel), sin embargo, en el caso de ser necesario o de requerirse se tendrá que presentar en las instalaciones del Instituto.<br>Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 456 de la empresa Scitum, S.A. de C.V. | Se presenta alguna las siguientes certificaciones vigentes:<br><br>CISM (Certified Information Security Manager)<br>CISSP (Certified Information Systems Security Professional)<br>CRISC (Certified in Risk and Information Systems Control) | 3 años de experiencia en participación de proyectos de seguridad de la información. | Responsable de la administración, monitoreo, operación de los servicios proporcionados por el SOC, así como del soporte, atención a fallas e incidentes de seguridad | Al menos 1 |

| Perfil | Certificaciones a demostrar | Experiencia a demostrar | Función | Numero de recursos |
|---|---|---|---|---|
| Administración y Operación de soluciones y herramientas tecnológicas<br><br>Operbes S.A. de C.V. tomó en consideración que el lugar de la prestación de servicio para este recurso y su esquema de atención ( remoto en el SOC de Bestel), sin embargo, en el caso de ser necesario o de requerirse se tendrá que presentar en las instalaciones del Instituto.<br>Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 457 de la empresa Scitum, S.A. de C.V. | Consultor especializado en cada una de las soluciones de seguridad integradas.<br>Operbes S.A. de C.V. tomó en consideración que Se aceptan como documentos comprobables el certificado vigente que haya tomado directamente del fabricante o de un centro de entrenamiento autorizado por el fabricante.<br>Operbes S.A. de C.V. tomó en consideración que las certificaciones solicitadas aplican para los Servicios de Seguridad - Continuidad Operativa:<br>- Servicios de Firewall<br>- Servicios de Prevención de Intrusos (IPS)<br>- Servicios de Protección contra Ataques Denegación de Servicio (DDoS)<br>- Servicios de Redes Privadas Virtuales (VPN)<br>- Servicios de Filtrado de Contenido Web<br>- Servicios de Filtrado de Contenido de Correo (Antispam)<br>- Servicios de Firewall Especializado en Servicios Web (WAF)<br>- Servicios de Firewall especializado en Base de Datos (DBF)<br>- Servicios de Gestión Unificada de Amenazas (UTM)<br>- Servicio de Correlación de Eventos<br>- Servicio de Protección de Amenazas Persistentes Avanzadas (APT).<br>Corresponden para la partida 1.<br>Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 316 de la empresa Operbes, S.A. de C.V. | 3 años de experiencia en participación de proyectos de seguridad de la información. | Operar administrar y monitorear las soluciones de seguridad propuestas. | Al menos 3 |

| Perfil | Certificaciones a demostrar | Experiencia a demostrar | Función | Número de recursos |
|---|---|---|---|---|
| Líder de proyecto | Se presenta alguna las siguientes certificaciones vigentes:<br><br>PMP (Project Manager Professional) Certificado por PMI<br>ITIL v4 (Expert o Master)<br>EC-Council Project Management In IT Security (PMITS) | 3 años de experiencia en participación de proyectos de seguridad de la información. | Es la persona encargada de administrar y coordinar el proyecto | Al menos 1 |
| Operador de la mesa de servicio SOC | Se presenta la siguiente certificación vigente:<br><br>ITIL v4 Foundation Certification | 3 años de experiencia en participación de proyectos de seguridad de la información. | Personal encargado de las operaciones de soporte de primer nivel, el monitoreo de los servicios, así como del registro y seguimiento de solicitudes de ventanas de mantenimiento, reportes de fallas y requerimientos | Al menos 4 |
| Arquitecto Especializado en Redes y Seguridad<br><br>Operbes S.A. de C.V. tomó en consideración el Arquitecto Especializado en Redes y Seguridad prestará sus servicios en sitio mayoritrimente de forma remota en el SOC de Operbes S.A. de C.V. y en sitio bajo demanda para la atención a fallas de incidentes que se presenten en la interoperabilidad, sin embargo, en el caso de ser necesario o de requerirse se tendrá que presentar en las instalaciones del Instituto.<br>Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 462 de la empresa Scitum, S.A. de C.V. | Se presenta alguna las siguientes certificaciones vigentes:<br><br>CCNP (Cisco Certified Network Professional)<br>CCIE Enterprise Infrastructure (Cisco Certified Internetwork Expert)<br>CCIE Security (Cisco Certified Internetwork Expert) | 3 años de experiencia en participación de proyectos de redes y seguridad de la información. | Responsable de la administración, monitoreo, operación de los servicios proporcionados por el SOC, en lo que a servicios de interconexión de red se refiere, así como del soporte, atención a fallas e incidentes que se presenten en la interoperabilidad con otros proveedores y/o fabricantes | Al menos 1 |

Operbes S.A. de C.V. tomó en consideración que este personal (página 5 a la 25 de la matriz de puntos y porcentajes todo el personal) es el mismo solicitado en este numeral y bastará que, Operbes S.A. de C.V.

haga la acreditación de esta información una solo vez siendo en la tabla de puntos donde se presente la información.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 119 de la empresa Axtel, S.A.B. de C.V.

Para dar cumplimiento con este punto favor de referirse a los documentos ubicados en el rubro I a). - Capacidad de los recursos humanos, surubro I a) 1.- Experiencia: en asuntos relacionados con la materia del servicio objeto del procedimiento de contratación, I a) 2.- Competencia o habilidad en el trabajo conforme a conocimientos académicos o profesionales dentro de la presente propuesta técnica y I a) 3.- Dominio de herramientas relacionadas con el servicio, dentro de la documentación proporcionada para la matriz de puntos y porcentajes.

**7. Condiciones técnicas de aceptación de entregables**

Durante la habilitación, transición y operación de los servicios de seguridad, Operbes S.A. de C.V. tomó en consideración que el Instituto requiere recibir distintos tipos de documentos, reportes, artefactos, dictámenes o esquemas que favorezcan el desempeño y la continuidad del servicio, y que den certidumbre a las actividades diarias que Operbes S.A. de C.V. efectuará bajo la supervisión de los funcionarios designados por este último para tales efectos.

**7.1. Entregables Generales**

Durante la habilitación, transición y operación de los servicios de seguridad, Operbes S.A. de C.V. tomó en consideración que el Instituto requiere recibir distintos tipos de documentos, reportes, artefactos, dictámenes o esquemas que favorezcan el desempeño y la continuidad del servicio, y que den certidumbre a las actividades diarias que Operbes S.A. de C.V. efectuará bajo la supervisión de los funcionarios designados por este último para tales efectos.

Operbes S.A. de C.V. tomó en consideración que los Entregables Generales solicitados en esta convocatoria, son los
entregables que serán entregados al inicio de la vigencia del contrato y considerados como entregables iniciales del proyecto.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 374 de la empresa Operbes, S.A. de C.V.

**Partida 1**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Habilitación, Operación y Transición | Plan de Trabajo Detallado de los servicios del proyecto | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Documento Compromiso de | Única Vez | |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | suscripción del acuerdo de niveles operacional (*Operational Level Agreement*, OLA) | | 15 días naturales posteriores a la emisión del fallo |
| | Matriz de Escalación | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Escrito por parte de Operbes S.A. de C.V. , firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| Servicios de Seguridad – Continuidad Operativa | Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto | Única Vez | 5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas | Única Vez | 10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo |
| | Memorias Técnicas Actualizadas de las | Única Vez | 20 días hábiles previo al término del contrato |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | Servicios de Seguridad | | para aquellos servicios que se encuentren habilitados |
| Servicios de Seguridad – Verificación/Calidad | Documento con el diseño de Alto Nivel de los servicios de Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integran activos de infraestructura para su habilitación | Única Vez | 5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integran activos de infraestructura para su habilitación | Única Vez | 10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo |
| | Memorias Técnicas Actualizadas de las Servicios de Seguridad, que requieran integran activos de infraestructura para su habilitación | Única Vez | 20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados |
| Servicios de Borrado Seguro de Información | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicio de Gestión de Dominios | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | | | integración de las mesas de trabajo |
| Servicio de Certificados Digitales SSL | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Sistema de Gestión de Seguridad de la Información (SGSI) | Metodología para la continuidad de los servicios | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Gestión del Cambio en Seguridad de la Información | Metodología para la implementación de los servicios | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Procesos de operación implementados:<br>• Requerimientos<br>• Cambios<br>• Configuraciones<br>• Incidentes<br>• Problemas<br>• Monitoreo | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Matriz de Escalación Técnica y Organizacional | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Procedimiento de operación de la Mesa de Servicios:<br>• Requerimientos<br>• Cambios<br>• Configuraciones<br>• Incidentes<br>• Problemas<br>• Monitoreo | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Expedientes Curriculares del personal del SOC | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| Tablero de Estadísticas de | Creación de cuentas de acceso en portal | Única Vez | |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Seguridad (Portal Único) | único de las soluciones de seguridad | | 10 días hábiles posteriores al término de la habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo |

Operbes S.A. de C.V. tomó en consideración que los "Procesos de operación implementados", refiere a todo aquellos mecanismos que demuestren a funcionalidad de un servicio y; "Procedimiento de operación de la Mesa de Servicios", refiere a la interacción de los servicios con el personal que da atención a los requerimientos.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 468 de la empresa Scitum, S.A. de C.V.

**7.2. Entregables bajo demanda**

Operbes S.A. de C.V. , de manera enunciativa más no limitativa, generará entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

Operbes S.A. de C.V. tomó en consideración que los entregables bajo demanda especificados en esta convocatoria, serán solicitados previamente por la convocante a los licitantes ganadores, mediante solicitud formal emitida por la convocante.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 375 de la empresa Operbes, S.A. de C.V.

**Partida 1.**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Borrado Seguro de Información | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado. | | |
| Servicio de Gestión de Dominios | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos. | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicio de Certificados Digitales SSL | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los certificados que se hayan renovado o adquiridos (incluyendo archivo electrónico compreso con la llave publica relacionado con los requerimientos) | Evento | 1 día hábil posteriores a la solicitud generada por parte del Instituto |
| Servicios de Sistema de Gestión de Seguridad de la Información | Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo | Evento | 10 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicios de Gestión del Cambio en Seguridad de la Información | Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo | Evento | 10 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad | Evento | 5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto |
| | Creación de cuentas de acceso en la base de conocimientos de | Evento | 5 días hábiles posteriores al término de la implementación de cualquier solución |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | las soluciones de seguridad | | de seguridad o conforme cada solicitud generada por el Instituto |
| | Actualización de la matriz de escalación | Evento | 5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad y Red |
| | Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad y red | Evento | 5 días hábiles posteriores a la ejecución de la ventana mantenimiento |
| | Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad y red | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Reporte Técnico de las configuraciones de las soluciones de seguridad y red | Evento | 5 días hábiles posterior a la solicitud generada por parte del Instituto |
| | Reporte Técnico de los incidentes presentados en las soluciones de seguridad y red | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Reporte Técnico de los requerimientos registrados en la mesa de servicios | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y red, así como su diagrama de interrelación conforme fueron registrados en la CMDB | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Diagramas de Arquitectura de las soluciones de seguridad y red | Evento | 2 días hábiles posteriores a la solicitud generada por parte del Instituto |

Operbes S.A. de C.V. tomó en consideración que los reportes indicados se refieren a un reporte con la relación de los requerimientos atendidos y finalizados en el periodo, y que estos no sustituyen a los entregables generados para cada requerimiento.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 209 de la empresa All Service In Telecom and Medice S. de R.L. de C.V.

### 7.3. Entregables Periódicos

Operbes S.A. de C.V. , de manera enunciativa más no limitativa, generará entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

### Partida 1

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Seguridad – Continuidad Operativa | Reportes Técnicos de los activos de infraestructura que contemplen:<br>• Disponibilidad<br>• Controles de Cambios<br>• Requerimientos<br>• Incidentes/Fallas<br>• Actividad Sospechosa<br>• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| Servicios de Seguridad – Verificación/Calidad | Reportes Técnicos de los activos de infraestructura que contemplen:<br>• Disponibilidad<br>• Controles de Cambios<br>• Requerimientos<br>• Incidentes/Fallas<br>• Actividad Sospechosa<br>• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte de las evaluaciones operativas a los servicios de seguridad implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |
| | Reporte que integre el calendario de actualizaciones de versionamiento en *software* de cada servicio implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |

Los entregables requeridos durante la vigencia del contrato, serán entregados en formato electrónico (MS Word, MS Excel, PDF) conforme los periodos estipulados por el Instituto.

De igual manera, Operbes S.A. de C.V. establecerá un repositorio digital, que, de manera alterna, servirá para alojar los entregables antes señalados, mismos que estarán disponibles para su consulta durante la vigencia del contrato, teniendo en cuenta que el Instituto definirá en las mesas de trabajo los permisos de acceso correspondientes para el administrador del contrato, cuerpo de gobierno que se conforme para este propósito u otros funcionaros que sean designados por el primero mencionado.

**8. Niveles de servicio que deberán cumplirse (SLA)**

Operbes S.A. de C.V. tomó en consideración que el objetivo de los Niveles de Servicio consiste en proporcionar al Instituto un mecanismo que permita:

- Medir de forma efectiva el desempeño de los servicios proporcionados por Bestel.
- Procurar que los servicios de sean proporcionados con la calidad prevista.

Los Niveles de Servicio son métricas definidas por el "IMSS" que serán cumplidas por Operbes S.A. de C.V. en cso de ser el proveedor de SASI 2022-2024, con objeto de cumplir con la calidad requerida en la prestación del servicio.

Con relación a lo establecido en los artículos 45, fracción XIX, 53 y 53 BIS de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 86, segundo párrafo, 95, 96 y 97 de su Reglamento; se aplicarán las Penas Convencionales y Deducciones correspondientes, por atraso en el cumplimiento de las fechas pactadas de entrega o de la prestación del servicio y, con motivo del incumplimiento parcial o deficiente en que pudiera incurrir Operbes S.A. de C.V. en caso de ser el "Proveedor" de SASI 2022-2024, respecto de los servicios prestados.

Los niveles de servicios se aplicarán conforme a lo estipulado en el documento de "Términos y Condiciones".

**8.1. Penas Convencionales**

Operbes S.A. de C.V. tomó en consideración que durante la vigencia del contrato, se aplicarán penas convencionales a todos aquellos servicios que no sean entregados conforme lo establecido en los niveles de servicios definidos por el instituto.

Las penas convencionales se aplicarán conforme a lo estipulado en el documento de "Términos y Condiciones".

**9. Deducciones**

Durante la vigencia del contrato, al presentarte una falla, incidente, atención de requerimientos, ventana de mantenimiento, entre otras, cuya causa raíz haya sido derivada por un tercero, la deductiva correspondiente al servicio asociado no será aplicada a Operbes S.A. de C.V. en caso de ser el proveedor de SASI 2022-2024, siempre y cuando demuestre con evidencias fehacientes que el servicio correspondiente se presentó bajo las especificaciones del anexo técnico y sus apéndices de las bases de la licitación.

Con base en lo anterior, y cuando las fallas, incidentes, atención de requerimientos, ventanas de mantenimiento, entre otras, sean atribuibles a la entrega de los servicios de seguridad por parte de Operbes S.A. de C.V. se aplicará una deductiva conforme los niveles de servicios establecidos,

Las deducciones se aplicarán conforme a lo estipulado en el documento de "Términos y Condiciones".

**10. Convenio de Confidencialidad y Resguardo de la Información**

Bestel, en caso de ser el licitante ganador, suscribirá el Convenio de Confidencialidad y Resguardo de Información correspondiente. En complemento, Operbes S.A. de C.V. considerará al menos los siguientes mecanismos de control de acceso a la información del IMSS:
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 615 de la empresa Totalsec, S.A. de C.V.

a. Se establecerá controles de acceso y privilegios restringidos al personal de Operbes S.A. de C.V. , a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del IMSS.

b. Operbes S.A. de C.V. implantará y aceptará en todo momento el uso de controles que permitan establecer "Pistas de Auditoria" para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.

c. Los empleados de Operbes S.A. de C.V. con acceso a la información sensible del IMSS, firmará acuerdos de confidencialidad con este.

d. Operbes S.A. de C.V. tomó en consideración que el almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por el instituto de los servicios de SASI 2022- 2024 observando los requisitos de seguridad y resguardo de la información.

e. Operbes S.A. de C.V. permitirá el acceso a información relacionada con el servicio prestado al IMSS para la realización de auditorías.

f. Operbes S.A. de C.V. no hará uso indebido de la documentación, información, ni activos de TIC a los que tengan acceso o que se generen con motivo de la prestación del servicio.

**11. Normas**

Operbes S.A. de C.V. tomó en consideración que no aplica

**12. Normatividad Aplicable**

Operbes S.A. de C.V. se sujetará a las políticas internas vigentes del Instituto y a cualquier modificación o inclusión de nuevas políticas que se realicen durante la vigencia del contrato. Operbes S.A. de C.V. tomó en consideración que las políticas aplicables se le darán a conocer durante las mesas de trabajo, sin embargo, se considerará las que se enlistan a continuación, de manera enunciativa más no limitativa:

- Marco normativo de aplicación general y obligatoria en la Administración Pública Federal.
- Artículo 8, segundo y tercer párrafo, fracción I de la Ley Orgánica de la Administración Pública Federal.
- Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la Información y comunicación, y la seguridad de la información en la Administración Pública Federal.
- Políticas de Seguridad con base en el Sistema de Gestión de Seguridad de la Información (SGSI) del Instituto.
- Certificados ISO/IEC27001:2013 e ISO/IEC20000-1:2018 vigentes a nombre de Operbes S.A. de C.V. .

**13. Cumplimiento de Políticas**

Operbes S.A. de C.V. respetará las políticas de seguridad vigentes en el Instituto y bajo ninguna circunstancia permitirá que se infrinjan los lineamientos vigentes. Si alguno de los lineamientos de seguridad implantados en el Instituto llegase a cambiar durante la vigencia del contrato establecido con dicho proveedor, éste se asegurará de modificar su infraestructura y procesos de tal forma que cumpla con los nuevos requerimientos.

Todos los equipos de cómputo personal propiedad de Operbes S.A. de C.V. , que estén involucrados en la prestación de los servicios, estará protegidos con sistemas de detección de intrusos, control de infecciones virales, detección y eliminación de programas tipo "back door" o "Troyanos". Operbes S.A. de C.V. tomó en consideración que esta regla aplica tanto para los equipos de cómputo móviles (laptops, handheld, smartphones, tablet PC, etc.) como para los equipos de escritorio (desktop, deskside, etc.) usados por los recursos designados para las diversas tareas de administración y gestión.

Si dichos equipos requieren de la instalación de sistemas operativos, aplicaciones, sistemas antivirus, sistemas de seguridad y demás herramientas que Operbes S.A. de C.V. considere necesario para la correcta

operación de su personal, así como de la adquisición, instalación, mantenimiento y licenciamiento de estos, el costo será absorbido por Operbes S.A. de C.V. .

**14. Finalización del Contrato**

En el caso de terminación anticipada del contrato o a la finalización de la vigencia del mismo, Operbes S.A. de C.V. será responsable de iniciar el proceso de respaldo de la información, el proceso de baja, de realizar los movimientos de resguardo, traslado y empaquetado de todo el equipo ubicado en las instalaciones del IMSS que forma parte de los servicios y que no constituya parte de las modificaciones, adecuaciones y/o activos que hayan sido realizados como permanentes, o aquellos que de común acuerdo con el IMSS hayan sido sustituidos como parte del servicio.

Una vez terminada la vigencia del servicio, la infraestructura, los componentes habilitadores y los demás elementos utilizados por Operbes S.A. de C.V. se transferirán al IMSS para la continuidad operativa. Este acto se llevará a cabo mediante un acta de entrega recepción, en la que dichos componentes se transmitirán al IMSS, a título gratuito, libres de toda limitación de dominio, gravamen y responsabilidad de cualquier naturaleza, conforme a la normativa aplicable al Instituto.

Operbes S.A. de C.V. entregará al IMSS, a más tardar 2 meses antes de la finalización del contrato, un plan de trabajo detallado para lograr una transición efectiva de los servicios de seguridad, en el que se incluyan todos aquellos elementos para efectuarlo. Dicho plan permitirá una completa y correcta transición de los servicios, incluyendo la conformación y actualización de la documentación necesaria del proyecto, así como las mesas de trabajo necesarias para dicha transición con el o los proveedores que den continuidad operativa al proyecto.

La documentación incluirá información que se generó durante la vigencia del contrato, documentación de los procesos internos de aprovisionamiento, configuración y tareas de operación, soporte y mantenimiento debidamente actualizadas, tomando en consideración los eventos de administración de cambios y configuración, incidentes y problemas, además de un inventario actualizado a la fecha de entrega de todos los componentes habilitadores e infraestructura auxiliar que el IMSS solicite se mantengan para la transición de un nuevo contrato de servicios, para que pueda continuarse prestando el mantenimiento preventivo y correctivo a todos los componentes de la solución y diseñar el mecanismo para la renovación tecnológica del resto, procurando afectar de forma mínima la operación.

La fecha límite para la entrega de la documentación final actualizada que se mencionó anteriormente será de 2 meses antes de la finalización del contrato SASI 2022-2024. Asimismo, Operbes S.A. de C.V. implementará un esquema de respaldo de la información en cada uno de los componentes que integran los servicios incluyendo los relacionados con los Centros de Datos del IMSS, el respaldo de la información será almacenada en cada punto táctico para ser entregada al cuerpo de gobierno del contrato para su resguardo. Una vez contando con la autorización del cuerpo de gobierno de SASI 2022-2024.

Asimismo, al término del contrato, garantizará los niveles de servicio durante el período de transferencia de servicios al nuevo proveedor.

Dicho período de transición estará sujeto al plan de trabajo que Operbes S.A. de C.V. haya presentado previamente, y que el IMSS hubiera aprobado. No obstante, durante dicho periodo, Operbes S.A. de C.V. proporcionará la orientación tecnológica adecuada al personal del IMSS para garantizar la continuidad de los servicios requeridos, poniendo a disposición del IMSS o de un tercero la transferencia.

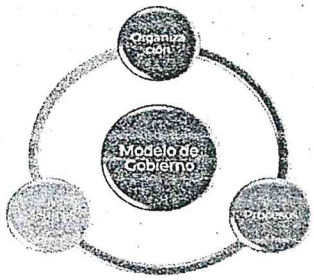
**15. Modelo de Gobierno**

El Modelo de Gobierno establece la forma como se trabajará en relación con este proyecto, los lineamientos operacionales para Operbes S.A. de C.V. y la manera como se medirá el grado de desempeño. El Modelo de Gobierno surge de la necesidad de diseñar una estructura operativa orientada a procesos para administrar los "Servicios Administrados de Seguridad Informática SASI 2022-2024", el cual facilitará la relación entre todos los involucrados para su adecuada implantación y operación.

El Modelo de Gobierno comprende los principales aspectos a considerar para asegurar y controlar la operación del proyecto.

Dicho modelo establece la organización y los roles que participarán por parte del Instituto dentro del proyecto.

El Modelo de Gobierno establece esquemas operativos y procesos, con la finalidad de que cada una de las etapas del servicio, el administrador del contrato y los líderes del proyecto, con apoyo por parte de Operbes S.A. de C.V. (SOC), garanticen los niveles de servicios establecidos para la operación.




Operbes S.A. de C.V. tomó en consideración que la estructura organizacional que ejecutar para el proyecto de "Servicios Administrados de Seguridad Informática (SASI 2022-2024)", busca que los responsables trabajen de manera efectiva, definiendo roles y responsabilidades en cada nivel, para lo cual se muestra en la siguiente tabla de manera enunciativa mas no limitativa a los responsables y sus roles correspondientes.

| NIVELES ORGANIZACIONALES | RESPONSABLES | DESCRIPCIÓN |
|---|---|---|
| Supervisión y Administración de los Servicios | • Administración de Contrato | Determinar los incumplimientos respecto a las penas convencionales y/o deductivas descritas en Anexo Técnico, Términos y Condiciones en el apartado "Acuerdos de Niveles de Servicio de SASIC"<br>Elaborar el dictamen de servicios, el cual deberá contener los servicios prestados a mes vencido, así como la identificación de los incumplimientos de los mismos. |
| Líder de Proyecto Proveedor (SOC) | • Líder del proyecto del proveedor | Entregar al administrador del contrato la documentación relativa a los servicios bajo su responsabilidad ("Reporte de Servicios Consolidado" y "Reportes de Niveles de Servicios" correspondientes). |
| Líder de Proyecto Operación | • Líderes de los Servicios del proyecto SASIC | Mantener la operación de los servicios de acuerdo a los niveles de servicio establecidos en descritas en Anexo Técnico, Términos y Condiciones en el apartado "Acuerdos de Niveles de Servicio de SASIC". |

# Apéndice "A"

## Servicios Administrados de Seguridad Informática (SASI) 2022-2024

### 1. Objetivo del Documento

Operbes S.A. de C.V. tomó en consideración que el objetico es elaborar el documento que contenga los requerimientos y las especificaciones técnicas y de calidad, así como el alcance de la adquisición, arrendamiento o servicio de TIC y SI que se pretenda contratar.

### 2. Servicio de Firewall

Especificaciones Técnicas:

- Cumplirá con el desempeño y capacidades considerando al menos las siguientes especificaciones:

| | Tipo 1 | Tipo 2 | Tipo 3 | Tipo 4 |
|---|---|---|---|---|
| Desempeño | 5 Gbps | 10 Gbps | 20 Gbps | 240 Gbps |
| Conexiones simultaneas por seg. | 1,000,000 | 2,000,000 | 4,000,000 | 32,000,000 |
| Conexiones nuevas por seg. | 50,000 | 125,000 | 200,000 | 1,000,000 |
| Paquetes por seg. | 1,000,000 | 3,000,000 | 5,000,000 | 30,000,000 |
| Interfaces 10GbE | 8 | 8 | 12 | 12 |

Operbes S.A. de C.V. tomó en consideración que Conexiones simultaneas por seg. se puede interpretar como sesiones concurrentes por segundo.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 510 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que Conexiones nuevas por segundo se puede interpretar como sesiones nuevas por segundo.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, re
pregunta 17 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que se proporcionara mínimo 2 y máximo 4 equipos tipo 4 para el centro de datos principal, ubicado en Morelia Michoacán (configuración en HA)

Operbes S.A. de C.V. tomó en consideración que la consola de administración que refiere se proporcionara nueva junto con el equipamiento nuevo de Firewall tipo 4, estos equipos se implementaran en el centro de datos de Morelia, Michoacán .
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 9 de la empresa Operbes, S.A. de C.V.

- Operbes S.A. de C.V. considera en su propuesta económica que las características de conexiones simultaneas por segundo se refiere a conexiones concurrentes por segundo.

- Incluirá un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
- Certificado por organismos de la industria como Common Criteria o ICSA Labs.
- Incluirá la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permitirá implementar reglas aplicadas a intervalos de tiempo específicos.
- Integrará listas de control de acceso basadas en dirección origen, dirección destino, protocolos, interfaces de red, puertos, URL destino, identidad, rangos de tiempo o periodo.
- Capacidad de agrupar objetos tales como direcciones IP, protocolos y puertos para la simplificación de configuración de políticas de seguridad.
- Capacidad de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con tiempo de espera agotado (timeout).
- Capacidad de implementar mecanismos de calidad de servicio tales como la asignación de ancho de banda a cada tipo de flujo, encolamiento prioritario y moldeado de tráfico (traffic shaping).
- Capacidad de inspeccionar tráfico FTP, HTTP, HTTPS, DNS, ICMP, RADIUS, SMTP y SNMP, H.323, SIP, RSTP, SNMP, entre otros.
  Operbes S.A. de C.V. tomó en consideración que el protocolo RSTP mencionado se refiere al protocolo RSTP (Rapid Spanning Tree) el cual se habilita en equipos switches por lo que no aplicaría para el servicio de Firewall y al que hace referencia es al protocolo RTSP que está orientado a conexión para servicios TCP Y UDP.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 473 de la empresa Scitum, S.A. de C.V.

- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Capacidad de segmentar lógicamente el o los activos de infraestructura en dispositivos virtuales (firewalls virtuales); en el que cada instancia virtual es un dispositivo independiente con sus propias políticas de seguridad, interfaces y usuarios administrativos.
- Capacidad de crear hasta 100 instancias de dispositivos virtuales (firewalls virtuales) que deberán ser soportadas en cada uno de los diferentes tipos de firewalls.
- soportará Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
- Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
- Soportará y operará bajo protocolos de ruteo BGP y OSPF.
- Soportará y operará mediante rutas estáticas.
- Realizará inspección en capa 3 y 4.
- Soportará y operará con al menos 1,000 VLANs
- Integrará esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Permitirá almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Contará y operará al menos con una interface Gigabit Ethernet dedicada para administración.
- Generación de bitácoras de eventos (logs) con múltiples niveles de criticidad.
- Incluirá una consola centralizada de gestión con las siguientes características:
  - Configuración, de manera centralizada, de políticas en todos los firewalls de la infraestructura.
  - Identificación de qué reglas corresponden a fuentes, destinos y tipos de tráfico.
  - Ejecución de operaciones para grupos o bloques de dispositivos de frontera de seguridad.

- Capacidad de ofrecer diferentes vistas durante el monitoreo de dispositivos, topologías o políticas.
- Agrupación de parámetros de configuración para su posterior implementación.

- Durante una actualización de configuración, será capaz de regresar a la configuración anterior, si es necesario o requerido.
- Auditoria de todas las actividades realizadas por los usuarios con privilegios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que incluirá fecha y hora de cada actividad realizada.

**3. Servicio de Prevención de Intrusos (IPS)**

Especificaciones Técnicas:

- Cumplirá con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

| | Tipo 1 | Tipo 2 | Tipo 3 |
|---|---|---|---|
| Desempeño | 15 Gbps | 20 Gbps | 24 Gbps |
| Conexiones simultaneas / concurrentes por seg. | 15,000,000 | 25,000,000 | 30,000,000 |
| Conexiones nuevas por seg. | 120,000 | 160,000 | 200,000 |
| Interfaces 10GbE | 4 | 8 | 8 |

Operbes S.A. de C.V. proporcionará mínimo 2 y máximo 4 equipos tipo 3 para el centro de datos Principal ubicado en Morelia Michoacán (configuración en HA)

Operbes S.A. de C.V. tomó en consideración que la consola de administración que refiere se proporcionara nueva junto con el equipamiento nuevo de IPS tipo solicitado, estos equipos se implementarán en el centro de datos de Morelia, Michoacán .
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 10 de la empresa Operbes, S.A. de C.V.

- Incluirá un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Latencia máxima de 0.5 milisegundos.
- Las interfaces de Inspección operarán en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
- Capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado.
- Capacidad de detección en línea sin bloquear tráfico (Modo transparente o supervisión). El sistema sólo alertará que eventos serían bloqueados.
- Capacidad de configuración del modo transparente o supervisión para todo el tráfico o sólo para los paquetes especificados por dirección IP, protocolo, VLAN ID, entre otros.
- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.
- Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
- Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.

- La solución de IPS contemplará que el flujo de información esté asegurado ante una falla en el IPS, pudiendo conmutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.
- Soporte de funcionalidades de alta disponibilidad y configuraciones del tipo activo/activo y activo/failover. Esto será soportado sin degradar el desempeño del IPS y manteniendo las tasas de transmisión requerida.
- Soporte de actualizaciones automáticas de seguridad del archivo de firmas de cuando menos una vez por mes.
- Soporte de análisis de tráfico de voz sobre IP.
- Soporte de monitoreo de VLANs, incluyendo tramas 802.1q
- Soporte de monitoreo de IPv6.
- Soporte de monitoreo con inspección profunda de paquete y monitoreo de paquete en escenarios de alta disponibilidad y con handshake TCP incompleto.
- Reconocimiento de Tuneleo de Protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
- Detección de escaneo de puertos.
- Detección de re-ensamblaje de paquetes fragmentados.
- Captura de tráfico para el análisis de evidencia en formato soportado por TCPDUMP y de manera opcional en formato. ENC (estándar para el software de análisis de protocolos), dicho archivo será usado para hacer reconstrucción o análisis forense del ataque.
- Integración de Listas Blanca (IP whitelist) mediante una lista de direcciones IP "confiables" que el sistema no bloqueará.
- Integración de firmas definidas por el Instituto mediante el uso de expresiones regulares.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos hosts de la red y crear una alarma cuando cierto umbral sea rebasado.
- Capacidad de integración con el directorio de usuarios (Active Directory y/o LDAP).
- Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
- Administración de seguridad centralizada que incluya las políticas, actualización, respuestas (bloquear, notificar, ignorar, etc.) y opciones de auditoría.
- Consola centralizada que administre los IPS y la integración de usuarios que realice las configuraciones necesarias para remediación de incidentes de seguridad.
- Consola remota con interfaz gráfica o Web cifrada (HTTPS) para el uso en modo de consulta, con diferentes perfiles de usuarios.
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que incluirá fecha y hora de cada actividad realizada.
- Soportará Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
- Capacidad de segmentar lógicamente el o los activos de infraestructura en dispositivos virtuales (IPS virtuales); en el que cada instancia virtual es un dispositivo independiente con sus propias políticas de seguridad, interfaces y usuarios administrativos.
- Operbes S.A. de C.V. considera en su propuesta económica la capacidad de crear hasta 100 instancias de dispositivos virtuales (IPS virtuales) en todos los equipos ofertados.
- Para los equipos en el centro de datos principal se requiere una consola de Administración.

**4. Servicios de Protección contra Denegación (DDoS)**

| | Tipo 1 | Tipo 2 |
|---|---|---|
| Desempeño | 20 Gbps | 120 Gbps |
| Conexiones simultaneas por seg. | 25,000,000 | 120,000,000 |
| Conexiones nuevas por seg. | 160,000 | 600,000 |
| Interfaces 10GbE | 8 | 8 |

Operbes S.A. de C.V. tomó en consideración que los parámetros definidos en la sección 'Conexiones Simultáneas por Seg.' se refieren a la capacidad de mitigación de la plataforma que se mide en paquetes por segundo (pps).
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 476 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. proporcionará mínimo 2 y máximo 4 equipos tipo 2 para el Centro de Datos Principal ubicado en Morelia Michoacán (configuración en HA)

Operbes S.A. de C.V. tomó en consideración que la consola de administración que refiere se proporcionara nueva junto con el equipamiento nuevo de Protección contra Denegación (DDoS) tipo 2 , estos equipos se implementaran en el centro de datos de Morelia, Michoacán .
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 11 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que el servicio será no sólo capaz de realizar el monitoreo en tiempo real, si no incluso contener el comportamiento anormal antes de que lleguen a los enrutadores implicados en los enlaces.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 21 de la empresa Totalsec, S.A. de C.V.

Especificaciones Técnicas:

Cumplirá con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluirá un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Operbes S.A. de C.V. considera en su propuesta que la cantidad de tráfico máximo a inspeccionar por lo equipos y un ancho de banda de los enlaces de internet que estarán recibiendo los equipos, de 1 Gbps para ambos casos.
  Operbes S.A. de C.V. tomó en consideración que se considera al menos un 1 Gbps de ancho de banda.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 648 de la empresa Totalsec, S.A. de C.V.

  Operbes S.A. de C.V. tomó en consideración que 1 Gbps será para todas las localidades incluido el Centro de Datos de Morelia.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 26 de la empresa Totalsec, S.A. de C.V.

- Garantizará el paso transaccional de datos legítimos, privilegiando la eliminación de tráfico anómalo dentro de los canales de comunicación del Instituto (Clean Pipes).

Operbes S.A. de C.V. tomó en consideración que se acreditara este punto en la propuesta técnica con la herramienta propuesta y no así con la carta de fabricante.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 652 de la empresa Totalsec, S.A. de C.V.

- Detección del tráfico basado en el lenguaje TCPDUMP (con información definida en las capas 3 y 4)
- Tendrá la capacidad de advertir anticipadamente algún posible ataque, analizando tendencias de tráfico malicioso en tiempo real.
- Tendrá capacidad de monitoreo en tiempo real de los circuitos dedicados que entregan la conectividad a Internet/Intranet para detectar el comportamiento anormal del tráfico que pueda estar dirigido a atacar las interfaces de los enrutadores implicados en los enlaces.
  Operbes S.A. de C.V. tomó en consideración que los ruteadores implicados en los enlaces soportan la creación de túneles GRE así como la utilización del protocolo BGP de enrutamiento hacia Internet
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 251 de la empresa Global Boga, S.A. de C.V.

  Operbes S.A. de C.V. tomó en consideración que para establecer los túneles GRE de la solución hibrida es necesario contar con ruteadores full routing, los cuales ya cuente la Convocante con estos equipos con la capacidad requerida.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 266 de la empresa Nelson Morgan Consulting, S.A. de C.V.

- Tendrá la capacidad de monitoreo en tiempo real las subredes pública que conectan los enlaces, para que permita la detección de tráfico anormal que pueda significar un ataque dirigida a ella.

  Operbes S.A. de C.V. tomó en consideración que las subredes públicas que conectarán los enlaces son de al menos una clase C.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 650 de la empresa Totalsec, S.A. de C.V.

- 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 un evento de tipo alerta, en paquetes por segundo y bytes por segundo.
- Soportará alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Capacidad de agrupar objetos tales como direcciones IP, protocolos y puertos para la simplificación de configuración de políticas de seguridad.
- Capacidad de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con tiempo de espera agotado (timeout).
- Monitoreará, de manera enunciativa más no limitativa, las siguientes variables en tiempo real:
  - Para el protocolo IP:
    - ICMP
    - Paquetes IP fragmentados
    - Paquetes IP NULL
    - Paquetes IP con direcciones privadas
  - Para el protocolo TCP:
    - Segmentos TCP NULL
    - Segmentos TCP RST
    - Segmentos SYN
    - Tráfico total
- Como mínimo detectará los siguientes tipos de ataques DoS/DDoS sobre las interfaces, subredes y activos de infraestructura:
  - ACK Flood
  - SYN Flood

- Hogging CPU
- Chargen (Character generator)
- FIN Flood
- ToS Flood
- DNS Malformed
- HTTP Flood
- ICMP Flood
- UDP Flood
- Non- UDP/TCP/ICMP Protocol Flood
- PPS Flood Attack
- Zombie attack
- Land Attack

- Permitirá la personalización de los niveles de alarma o umbrales que sirvan para la detección de ataques, a una granularidad por objeto monitoreado.
- Monitoreará actividad sospechosa que pueda significar algún ataque de gusanos, virus, entre otros.
- Monitoreará actividad "Dark IP".
- Detección de anomalías DDoS y amenazas de día cero antes de que impacten en los servicios.
- Detección de zombis (con selecciones de umbrales en bytes por segundos y paquetes por segundos) para clasificar una IP como zombis y con la opción de conocer una lista de zombis activos detectados.
- Protección contra amenazas conocidas
  - Ping de la muerte
  - Ataque por inundación SYN
  - Fragmentación de paquetes y reensamblaje
  - Broadcast de correo electrónico
  - Saturadores de CPU
  - Scripts generadores de trafico
  - Generadores de caracteres
  - Ataques fuera de banda (WinNuke)
  - Ataque Smurf (generador de gran cantidad de paquetes ICMP)
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluye al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que incluirá fecha y hora de cada actividad realizada.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

**5. Redes Privadas Virtuales – VPN (C2S – S2S)**

Operbes S.A. de C.V. proporcionará mínimo 1 y máximo 2 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuración en HA)

Operbes S.A. de C.V. tomó en consideración que cuando dice mínimo 1 se proporcionará en realidad 2 equipos por la solicitud de configuración en HA, se implementará para las configuraciones en HA máximo 2 equipos
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 287 de la empresa Operbes, S.A. de C.V.
Operbes S.A. de C.V. tomó en consideración que la consola de administración que refiere se proporcionara nueva junto con el equipamiento nuevo de Redes Privadas Virtuales-VPN (CS2-S2S) , estos equipos se implementarán en el centro de datos de Morelia, Michoacán .

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 12 de la empresa Operbes, S.A. de C.V.

Especificaciones Técnicas:

Cumplirá con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluirá un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Incluirá al menos 4 interfaces 10/100/1000 Gb, expandibles a interfaces 10Gb de ser necesario.
  Operbes S.A. de C.V. tomó en consideración que se acepta que la solución cuente con al menos 2 interfaces de 10GE integradas adicional a los puertos de 4 puertos de 1GE, sin que este cuente con módulo de expansión
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 511 de la empresa Scitum, S.A. de C.V.

- Tendrá un desempeño de al menos 2Gbps y 1,000,000 conexiones concurrentes
  Operbes S.A. de C.V. tomó en consideración que la referencia de desempeño está relacionada con los activos de infraestructura que dan servicio a redes privadas virtuales VPN (C2S – S2S). Al menos 5000 C2S y S2S
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 76 de la empresa Axtel, S.A.B. de C.V.

- Capacidad de permitir 50,000 nuevas conexiones por segundo.
- Incluirá la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permitirá implementar reglas aplicadas a intervalos de tiempo específicos.
- Soportará alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Integrará esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Permitirá la creación de grupos de usuarios.
- Permitirá delimitar la cantidad de conexiones por usuarios.
- Permitirá almacenar una base de usuarios local que permita realizar autenticación, sin depender de un servicio de autenticación externo.
- Capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
- Soportará DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKEv2.
- Soportará al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Soportará integridad de datos con md5, sha1 y sha2.
- Soportará las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Establecerá VPNs con gateways con direcciones IP dinámicas públicas.
- Creará una única asociación de seguridad (SA) por par de redes o subredes.
- Realizará VPNs SSL.
  Operbes S.A. de C.V. tomó en consideración que se proporcionara al menos 5,000 VPNs SSL.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 2 de la empresa Adserti, S.A. de C.V.

- Soportará la conexión desde dispositivos móviles y de escritorio a través de un cliente de acceso remoto. Dicho cliente soportará al menos las siguientes plataformas operativas: MAC OS X desde v10.4.10, iOS desde v4, Android desde v4.2, Windows desde v7.

  Operbes S.A. de C.V. tomó en consideración que la versión Mac OS X 10.4.10 fue liberada en junio de 2007 y que el fabricante recomienda la actualización a Mac OS 10.13, el cliente de acceso remoto tendrá soporte para la versión 10.13 conforme a las recomendaciones en materia de seguridad.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 477 de la empresa Scitum, S.A. de C.V.

  Operbes S.A. de C.V. tomó en consideración que la versión la versión iOSv4 fue liberada en junio de 2010 y que el fabricante recomienda la actualización a iOS v6, el cliente de acceso remoto tendrá soporte para la versión 6 conforme a las recomendaciones en materia de seguridad.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 478 de la empresa Scitum, S.A. de C.V.

**6. Filtrado de Contenido Web**

Cumplirá con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluirá un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
  Operbes S.A. de C.V. tomó en consideración que el filtrado de contenido Web proporcionará protección e inspección de tráfico tanto en dispositivos de escritorio como en dispositivos móviles.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 77 de la empresa Axtel, S.A.B. de C.V.
  Operbes S.A. de C.V. tomó en consideración que el número de buzones onpremise al menos son 80,000 y en la nube al menos 100.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 14 de la empresa Axtel, S.A.B. de C.V.

- Soportará de forma mínima 120,000 usuarios de forma simultánea.

  Operbes S.A. de C.V. tomó en consideración que el servicio estará dimensionado para soportar hasta 120,000 usuarios de forma simultánea, mismas que se relacionan con sesiones concurrentes.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 512 de la empresa Scitum, S.A. de C.V.

  Operbes S.A. de C.V. tomó en consideración que la cantidad de equipos para la solución de Filtrado de Contenido Web dependerán de la arquitectura, y capacidades de equipos y/o clústeres propuestos para la entrega de servicio y métricas solicitadas siempre y cuando se cumpla con las capacidades requeridas por la convocante.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 513 de la empresa Scitum, S.A. de C.V.

- Integrará esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
  Operbes S.A. de C.V. tomó en consideración que la solución de filtrado de contenido web opera actualmente en el Centro de Datos de San Luis Potosí, misma que está configurada en un esquema de Alta Disponibilidad (HA).
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 79 de la empresa Axtel, S.A.B. de C.V.

- Permitirá operar en modo de proxy explicito y/o proxy transparente.
- Mecanismos de autenticación tales como: archivos locales de contraseña NTLM, LDAP, RADIUS, Active Directory y certificados.
- Control de autenticaciones simultáneas con una misma cuenta de usuario.
- Cifrado de datos (usuario/contraseña) en el proceso de autenticación.
- Controlará e inspeccionará al menos los protocolos: HTTP, HTTPS (SSL), FTP, CIFS, MAPI, DNS, P2P, SOCKS (v4/v5), IM (AOL, MSN, Yahoo Messengers), TCP-Tunnel, MMS, RTSP.
  Operbes S.A. de C.V. tomó en consideración que LA CONVOCANTE permite el cumplimiento opcional debido a que algunos de los protocolos que solicita son protocolos de red interna y no aplican a un servicio de filtrado web que por definición es una protección de frontera hacia el exterior, sin embargo, HTTP, HTTPS se cumplirán de manera forzosa.

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 479 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que dado que SOCKS v5 es una evolución del protocolo SOCKS v4, de acuerdo pública con información pública de la IETF (https//tools.ietf.org/html/rfc1928), se dará cumplimiento demostrando el soporte del protocolo SOCKS v5
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 514 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que para protocolo MAPI, y de acuerdo con información pública de fabricante (https://social.technet.microsoft.com/wiki/contents/articles/S64.exchange-2010-clientaccess-
serverconfrgurestatic-rpc-ports.aspx), se está haciendo referencia al puerto 135.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 515 de la empresa Scitum, S.A. de C.V.

- Catalogará las páginas por dominio (o subdominio), URL o IP.
- Bloqueo de las amenazas emergentes más comunes como: pop-ups, banners, spyware, adware, compartición de archivos punto a punto (P2P file sharing).
- Clasificación en tiempo real de sitios en internet (on-the-fly) que aún no han sido asignados a alguna categoría (servicio automático de validación en línea del sitio para determinar si es malicioso en caso de no tenerlo asignado en alguna categoría).
- Monitoreo y bloqueo de aplicaciones P2P tales como: BitTorrent, eDonkey, Gnutella, Fasttrack.
- Permitirá personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
- Permitirá la clasificación de URL (dominio o subdominio) o IP en una sola categoría.
- Permitirá el uso de expresiones regulares.
- Permitirá la creación de categorías de filtrado personalizadas, así como la creación de listas blancas y negras de filtrado URL.
- Capacidad de evitar la ejecución de códigos maliciosos.
- Bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.
- Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).
- Permitirá la recopilación (caching) de páginas web en disco duro y memoria RAM, con el fin de hacer más eficiente el uso de los recursos del equipo.
- Proporcionará capacidades de administración y reporteo centralizado incluyendo control de acceso discrecional, control de versiones, auditoria de usuario, sistema y utilerías de restauración de configuración.
- Proporcionará soporte de administración multisesión (múltiples administradores utilizando el servicio de administración centralizado), a través de una interfaz gráfica vía Web cifrada (HTTPS).
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que incluirá fecha y hora de cada actividad realizada.

**7. Servicios de Filtrado de Contenido de Correo (Antispam)**

Cumplirá con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluirá un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Capacidad de hasta 1.5M de correos por hora
  Operbes S.A. de C.V. tomó en consideración que el dato de 1,500,000 de correos por hora es durante el horario de trabajo de oficina (de las 9:00 horas a las 17:00 horas) considerando el despliegue en el Centro de Datos Principal por lo que la capacidad de correos a procesar por la solución de antispam es de 1,500,000 x 8 horas, es decir entre 12 o 13 millones de correos diarios.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 480 de la empresa Scitum, S.A. de C.V.

- Con una capacidad de por lo menos 120,000 usuarios
- 12 TB por equipo, en HA por lo menos 24 TB.
  Operbes S.A. de C.V. tomó en consideración que se podrán proponer clústeres de equipos a fin de cubrir las capacidades necesarias para la provisión del servicio, considerando arquitecturas que garanticen la continuidad operativa conforme a los niveles de servicio establecidos en la CONVOCATORIA.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 481 de la empresa Scitum, S.A. de C.V.

- Integrará esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
  Operbes S.A. de C.V. tomó en consideración que la solución de filtrado de contenido de correo opera actualmente en el Centro de datos de San Luis Potosí, misma que está configurada en un esquema de Alta Disponibilidad (HA).
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 80 de la empresa Axtel, S.A.B. de C.V.

  Operbes S.A. de C.V. tomó en consideración que la cantidad de buzones a proteger será al menos 80,000 buzones.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 81 de la empresa Axtel, S.A.B. de C.V.

  Operbes S.A. de C.V. tomó en consideración que actualmente se encuentra implementado un servicio hibrido.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 82 de la empresa Axtel, S.A.B. de C.V.

- Capacidad de revisar tanto el correo entrante como el saliente.
- Escaneará y analizará el asunto, encabezados y el cuerpo de los correos recibidos y enviados.
- Contará con un filtro de contenido para buscar palabras clave en el cuerpo del mensaje, en los encabezados From, To, CC, Subject y en X-Headers. Así mismo, deberá poder detectar estas palabras en archivos adjuntos.
- Capacidad para poder configurar el tamaño máximo del mensaje y el número de destinatarios del correo tanto a nivel de conexión SMTP, como en políticas cuando el correo ya ha sido recibido.
- Contará con mecanismos para clasificar los remitentes por su origen y tomar decisiones de flujo y volumen en consecuencia. Además, se contará con la facilidad de designar ciertas fuentes de correo en grupos como listas negras, listas blancas o cualquier otro grupo al que deba aplicársele una política específica.

- Capacidad para ofrecer el análisis de archivos comprimidos en los formatos más populares, incluyendo aquellos con 7 capas de compresión.
- Capacidad de detectar el verdadero formato de un archivo y permitir aplicar políticas basadas en este rubro.
- Capacidad para detectar enlaces maliciosos dentro de los correos recibidos en base a la reputación de la URL, utilizando la tecnología de reputación del fabricante, permitiendo la configuración de umbrales para esta detección.
- Contará con un módulo de bloqueo de correo electrónico no deseado con base en la reputación de cuentas de correo, dominios y direcciones IP.
- Capacidad para soportar la revisión de firmas DKIM en los encabezados de correos entrantes.
- Contará con actualizaciones para sus patrones y motores de detección de spam (heurística), phising y código malicioso.
- Capacidades de colaboración con los centros de investigación de amenazas del fabricante, con la finalidad de reportar de manera automática cualquier comportamiento sospechoso relacionado con el tráfico de correo electrónico.
- Capaz de recibir tráfico con conexiones seguras (TLS) y poder hacer conexiones con otros servidores bajo el mismo protocolo.
- Contará con mecanismos que permitan evitar la recepción de correos de notificaciones dirigidas a cuentas de usuarios no válidos o que no existen en el dominio destino (correos de rebote o Bounced Mails).
- Bloqueo automático de IP debido a alta cantidad de envío de spam, ataque tipo DHA (Directory Harvest Attack), Bounced Mails o código malicioso, totalmente parametrizable al número de mensajes recibidos en un intervalo de tiempo determinado a discreción.
- Capacidad para Integrar excepciones, tanto en hosts remitentes como en destinatarios, así como para cuentas de usuarios o dominios específicos.
- Permitirá la creación de cuarentenas o carpetas de auditoría de correo, la cuarentena debe poder ser almacenada por la solución como mínimo 30 días.
- Cuando se encuentre contenido malicioso en cuerpo del correo y archivos adjuntos, podrá realizar cualquiera de las siguientes acciones:
  - Reemplazar texto del mensaje afectado.
  - Poner en cuarentena el mensaje completo.
  - Eliminar el mensaje completo.
  - Hacer copia de seguridad (copia del mensaje), para reportarlo con los centros de investigación de amenazas del fabricante.
- Detectará correos masivos con virus y removerlos además de los archivos adjuntos, incluyendo la característica de archivos adjuntos Zero-byte.
- Proporcionará la facilidad de enviar notificaciones a los usuarios (cuentas de correo electrónico) cuando algún evento sospechoso sea detectado.
- Capacidad de integrar agentes que realicen la función de escaneo y detección de spam en activos de infraestructura o servicios de correo electrónico bajo plataformas operativas Linux y/o Windows.

- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que incluirá fecha y hora de cada actividad realizada. Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

**8. Firewall Especializado en Servicios Web (WAF)**

Se proporcionará mínimo 1 y máximo 2 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuración en HA)

Operbes S.A. de C.V. tomó en consideración que cuando dice mínimo 1 se proporcionará en realidad 2 equipos por la solicitud de configuración en HA, se implementará para las configuraciones en HA máximo 2 equipos
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 289 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que se deberá considerar al menos 80 aplicaciones web.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 486 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que la cantidad de tráfico limpio (Throughput de inspección) máximo a considerar para el servicio de WAF en el centro de datos será al menos 5 Gbps.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 487 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que serán al menos 8 interfaces a 10 Gbps-SR.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 488 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que la consola de administración que refiere se proporcionara nueva junto con el equipamiento nuevo de Firewall Especializado en servicios Web (WAF), estos equipos se implementarán en el centro de datos de Morelia, Michoacán .
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 13 de la empresa Operbes, S.A. de C.V.

Especificaciones Técnicas:

Cumplirá con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluirá un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Integrará esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Inspección y análisis de perfiles de comportamiento normal de usuarios para detectar y mitigar el uso anormal de aplicativos Web.
- Soportará un throughput de 5 Gbps en capa 7.
- Soportará 100,000 Transacciones por Segundo (TPS).
- Operbes S.A. de C.V. en caso de ser el licitante ganador considera en su propuesta en términos de transacciones por segundo de tráfico HTTPS requiriendo PFS/DH (Perfect Forward Secrecy/ Diffie-Hellman) al menos 60,000 tps
  Operbes S.A. de C.V. tomó en consideración que el ancho de banda puro necesario a proteger para todos os sitios combinados al menos 1 Gb.

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 83 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que el ancho de banda máximo a proteger para este servicio será 5 Gbps.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 27 de la empresa Totalsec, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que los sitios a proteger será al menos 80 sitios.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 84 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que el balanceo de tráfico puede ser ejecutado desde la solución Onpremise en combinación con un servicio de nube (hibrido).
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 85 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que el balanceo de tráfico puede ser ejecutado desde la solución onpremise en combinación con un servicio de nube (hibrido)
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 27 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que es necesario considerar prevención de ataques tipo DDoS para los sitios protegidos.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 86 de la empresa Axtel, S.A.B. de C.V.

- Servicio de reputación para identificar y bloquear ataques automatizados y/o usuarios maliciosos.
- Detección de ataques por clientes automatizados y robots.
- Detección de URL rewriting u ofuscación del URL.
- Manejo de errores y reescritura de errores para aplicativos Web.
- Capacidad para soportar inspección del protocolo XML.
- Certificado por organismos de la industria como ICSA Labs o PCI.
- Actualización automática de firmas de prevención contra código malicioso.
- Parcheo sobre aplicativos Web contra vulnerabilidades nuevas o conocidas (parcheo virtual).
- Protección contra ataques/vulnerabilidades conocidas (OWASP), de manera enunciativa más no limitativa:
    - SQL injection
    - Cross Site Scripting
    - Cross Site Request Forgery
    - Sensitive Data Exposure
    - Security Misconfiguration
    - Broken Authentication and Session Management
    - Otras nuevas identificadas por OWASP
- Soportará formatos de mensaje:
    - Web 2.0
      Operbes S.A. de C.V. tomó en consideración que se acepta AJAX, JSON, XML como 'formato de mensaje' para web 2.0, ya que, al ser un concepto, no existe un formato de mensaje estandarizado, sino herramientas que utiliza.
      Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 490 de la empresa Scitum, S.A. de C.V.
    - HTML

- XHML
  Operbes S.A. de C.V. tomó en consideración que se acepta que por XHML se refiere tanto de XML como HTML por la plataforma.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 491 de la empresa Scitum, S.A. de C.V.
- HTML5
- XML
- JSON
- AJAX
- FLASH
- JavaScript.

- Soportará Protocolos: TCP v4 y v6, HTTP, HTTPS, SSL/TLS.
- Soportará mitigación de amenazas:
  - HTML Content Aware
  - Intrusion Detection and Prevention (URI patterns)
  - URI rate-based heuristics
  - Vendor Vulnerabilities
  - URL cloaking / rewrite
  - Parameter Inspection
  - Learning mode
- Integridad de transacciones:
  - Session Tracking Cookies, Source/Destination IPs
  - HTTP RFC conformance
  - HTML Form parameter checking
  - Cross-Site Scripting
  - Cookie Signing
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Soportará Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
- Operbes S.A. de C.V. considera en la presente propuesta al menos 200 sitios/portales a proteger.

**9. Servicios de Gestión Unificada de Amenazas (UTM)**

Especificaciones Técnicas:

Cumplirá con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

| | Tipo 1 | Tipo 2 | Tipo 3 | Tipo 4 |
|---|---|---|---|---|
| Desempeño | 1 Gbps | 2 Gbps | 5 Gbps | 10 Gbps |
| Conexiones nuevas por seg. | 10,000 | 20,000 | 50,000 | 100,000 |
| Conexiones simultaneas por seg. | 150,000 | 500,000 | 1,000,000 | 2,000,000 |
| Interfaces 10/100/1000 Mbps. | 4 | 4 | 8 | 8 |

Operbes S.A. de C.V. tomó en consideración que la tabla de especificaciones referente a las conexiones simultaneas y conexiones nuevas los valores están invertidos.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 254 de la empresa Global Boga, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que la referencia de desempeño está relacionada con paquetes o conexiones por segundo. Al menos 5000 C2S y S2S.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 88 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. proporcionara mínimo 1 y máximo 2 equipos tipo 4 para el centro de datos principal ubicado en Morelia Michoacán (configuración en HA)
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, Precisión 1 por parte de la Convocante.

Operbes S.A. de C.V. tomó en consideración que el tipo de UTM que requiere para el sitio de Michoacán es tipo 4.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 89 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que cuando dice mínimo 1 se proporcionará en realidad 2 equipos por la solicitud de configuración en HA, se implementará para las configuraciones en HA máximo 2 equipos
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 291 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que la consola de administración que refiere se proporcionara nueva junto con el equipamiento nuevo de Gestión Unificada de Amenazas (UTM) tipo 4, estos equipos se implementarán en el centro de datos de Morelia, Michoacán .
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 14 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. considera en la presente propuesta que funcionalidad de alta disponibilidad modo Activo/activo y/o Activo/Pasivo.

Operbes S.A. de C.V. considera en la presente propuesta que la característica de conexiones simultaneas por segundo" y "conexiones nuevas por segundo, se refiera a conexiones concurrentes por segundo, así así como considera que la suma de las sesiones concurrentes refiere a el servicio UTM por cada tipo y las sesiones concurrentes de la tabla de UTM.

Generales

- Incluirá un sistema operativo endurecido propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Soportará alta disponibilidad en modo Activo/Activo y Activo/Pasivo.

Funcionalidad Firewall

- Estará basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.

- Incluirá la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permitirá implementar reglas aplicadas a intervalos de tiempo específicos.
- Soportará y operará bajo protocolos de ruteo BGP y OSPF.
- Soportará y operará mediante rutas estáticas.
- Realizará inspección en capa 3 y 4.

Funcionalidad IPS e IDS

- Soporte de al menos: 1,000,000 conexiones simultáneas por cada Gigabit de inspección.
  Operbes S.A. de C.V. tomó en consideración que este punto de 1,000,000 conexiones simultáneas por cada Gigabit de inspección, la Convocante se refiere a conexiones concurrentes por segundo.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 517 de la empresa Scitum, S.A. de C.V.

- Latencia máxima de 0.5 milisegundos.
- Las interfaces de Inspección operarán en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
- El equipo será capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado
- Capacidad de detección en línea sin bloquear tráfico (Modo transparente). El sistema sólo alertará que eventos serían bloqueados.
- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.
- Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
- Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.
- La solución de IPS contemplará que el flujo de información esté asegurado ante una falla en el IPS, pudiendo conmutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.
- Reconocimiento de tuneleo de protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
- Detección de re-ensamblaje de paquetes fragmentados.
- integración de listas blanca (IP whitelist) mediante una lista de direcciones IP "confiables" que el sistema no bloqueará.
- Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos hosts de la red y crear una alarma cuando cierto umbral sea rebasado.

Filtrado de Contenido Web

- Permitirá operar en modo de proxy explicito y/o proxy transparente.
- Controlará e inspeccionará al menos los protocolos: HTTP, HTTPS (SSL).
- Catalogará las páginas por Dominio (o subdominio), URL o IP.
- Permitirá personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
- Permitirá la creación de categorías de filtrado personalizadas, así como la creación de listas blancas y negras de filtrado URL.
- Capacidad de evitar la ejecución de códigos maliciosos.
- Permitirá el bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.
- Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).

Funcionalidad VPN

- Incluirá la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permitirá almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
  Operbes S.A. de C.V. tomó en consideración que se considerará al menos 5,000 usuarios por sitio.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 518 de la empresa Scitum, S.A. de C.V.

- Soportará DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKE v2.
- Soportará al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Soportará integridad de datos con md5, sha1 y sha2.
- Soportará las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Establecerá VPNs con gateways con direcciones IP dinámicas públicas.
- Creará una única asociación de seguridad (SA) por par de redes o subredes.
- Soportará Secure Sockets Layer (SSL) versión 3, con al menos los siguientes algoritmos de cifrado simétrico y longitud de llaves: RC4 (128 bits) y 3DES (192bits).
  Operbes S.A. de C.V. tomó en consideración que el algoritmo de cifrado RC4(128 bits y el 3DES(192bits) se pueden sustituir por el algoritmo (AES128-AES192-AES256)
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 5 de la empresa Adserti, S.A. de C.V.

**10. Firewall Especializado en Base de Datos (DBF)**

Operbes S.A. de C.V. proporcionará mínimo 1 y máximo 2 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuraciones en HA)

Operbes S.A. de C.V. tomó en consideración que la consola de administración que refiere se proporcionara nueva junto con el equipamiento nuevo de firewall Especializado en base de datos (DBF), estos equipos se implementarán en el centro de datos de Morelia, Michoacán .
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 15 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que cuando dice mínimo 1 se proporcionará en realidad 2 equipos por la solicitud de configuración en HA, se implementará para las configuraciones en HA máximo 2 equipos
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 293 de la empresa Operbes, S.A. de C.V.

Especificaciones Técnicas:

- Tecnología de autoaprendizaje con mínima intervención humana, el proceso será constante y aprenderá estructura de bases de datos, incluyendo schemas, objetos, tablas; sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario.
  Operbes S.A. de C.V. tomó en consideración que la cantidad de servidores será de 10 servidores en una combinación de físicos o virtuales. Las capacidades de procesamiento oscilan entre 4 a 24 procesador de cuatro núcleos.
  Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 90 de la empresa Axtel, S.A.B. de C.V.

- Operará a nivel local y en la capa de red
- Soportará al menos los siguientes motores de Bases de Datos:
  - Microsoft SQL Server
  - Oracle
  - Sybase
  - Informix
  - MySQL
  - Progress
  - PostgreSQL
- Proporcionará protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.
- En caso de ser necesario la utilización de agentes, estos soportarán al menos los siguientes Sistemas Operativos:
  - AIX
  - HP-UX
  - Solaris
  - RHEL
  - SusE
  - OEL
  - Windows 32/64 bits
- Capacidad para funcionar independiente a la activación de la auditoría nativa de la base de datos.

- Transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
- Se proporcionará un repositorio para el registro de la actividad, el cual no será accesible por ningún otro mecanismo que no sea la interacción mediante la GUI (interfaz gráfica) proporcionada por el fabricante o por medios administrativos debidamente asegurados.
- Capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de comunicación, y configuración de seguridad, sin importar el sistema operativo sobre el que se encuentren instaladas.
- Capacidad para poder realizar descubrimientos automatizados en la red para identificar nuevas bases de datos siendo habilitadas, ya sea a nivel de servidor o puertos habilitados en servidores conocidos.
- Capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo a las políticas de negocio. Las definiciones de tipo de dato podrán crearse de manera flexible y granular.
- Capacidad para proveer un servicio de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.
- Apoyará en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y Control de cambios.
- Monitoreará toda la actividad de las bases de datos, y almacenará los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
- Monitoreará e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, ligas, stored procedures, entre otros.
- Hará análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.
- Capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.
- Capacidad para proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tendrá la facilidad de cambiar una política desde la alerta.
- Manejará reglas y políticas tan amplias o granulares como se requieran y podrá ser construidas automática o manualmente y podrá ser actualizadas, igualmente, de forma manual o automática.
- Las políticas granulares para control de acceso o generación de alertas contará con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios podrán usarse en cualquier número y cualquier combinación:
    - Número de registros a regresar por la consulta (SQL Query)
    - Número de registros afectados
    - Tipo de datos accesado (financiero, recursos humanos, inventarios, o cualquier definición personalizada)
    - Acceso a datos marcados como sensibles
    - Base de Datos, Schema, Instancia, Tabla y Columna accesada
    - Estado de autenticación de la sesión
    - Usuario y/o Grupo de Usuarios de Base de Datos conectado
    - Usuario conectado en la capa aplicativa, a diferencia del usuario conectado a la DB
    - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier customización por expresiones regulares)
    - Logins, Logouts, Queries
    - IPs de origen y destino
    - Nombre de Host origen, Usuario firmado en el Host origen
    - Aplicación usada para la conexión a la base de datos
    - Tiempo de respuesta/procesamiento del query
    - Errores en el manejador de SQL
    - Número de ocurrencias en intervalos de tiempo definidos
    - Por operaciones básicas (Select, Insert, Update, Delete)
    - Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export)



ANEXOS
DIVISIÓN DE CONTRATOS

- Por Stored Procedure o Function utilizada
- Si existe ticket asignado de cambios
- Hora del Día

- Posibilitará los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.
- Protegerá contra ataques SQL y no-SQL.
- Contará con un mecanismo de actualización de la inteligencia interna de seguridad, que incluye las pruebas de las evaluaciones de vulnerabilidad, las firmas contra ataques, la granularidad de las políticas de seguridad y defensas contra comportamientos conocidos.
- Considerará de emergencia, para potenciales violaciones de la información que incluyan, enunciativa más no limitativamente:
  - Altos volúmenes de acceso a datos sensibles más allá de lo habitual.
  - Acceso a datos inusual para cierta hora del día.
  - Acceso a datos desde una ubicación (física) desconocida.
  - Acceso a datos utilizando aplicaciones/herramientas no autorizadas.
- Manejará una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.
- Tendrá facilidades de Archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP)
- Tendrá la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.
- Contará con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual presentará la documentación respectiva en el descubrimiento de las mismas.
- Soportará y aplicará simultáneamente un modelo de seguridad positivo y negativo.
- El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que además cumplirá con las siguientes especificaciones:
  - Deberá bloqueará las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
  - Incluirá una lista pre-configurada y detallada de las firmas de ataque.
  - Permitirá la modificación o adición de firmas por el administrador.
  - Permitirá la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
  - Detectará ataques conocidos a nivel base de datos
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Soportará Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).

**11. Servicio de Correlación de Eventos**

Operbes S.A. de C.V. proporcionará mínimo 2 y máximo 4 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuraciones en HA)

Operbes S.A. de C.V. tomó en consideración que la cantidad de EPS a correlacionar es de al menos 10,000 eventos por segundo.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 93 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que se considerarán colectores de eventos, siendo al menos 2 activos de infraestructura. Las localidades donde se podrán ubicar los servicios son:
Ciudad de México
San Luis Potosí, San Luis Potosí
Monterrey, Nuevo León
Morelia, Michoacán
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 295 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que la cantidad mínima de equipos (2) equivale a dos dispositivos de colección
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 20 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que la cantidad de los equipos de Gestión, correlación y administrador de logs dependerán de los licitantes consideren conveniente, siempre apegándose a los requerimientos y las funcionalidades técnicas requeridas.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 21 de la empresa Scitum, S.A. de C.V.

Especificaciones Técnicas:

- Capacidad para recolectar datos de toda aplicación o dispositivo que tenga una fuente de eventos necesaria para la organización, siendo esto a través de desarrollos predefinidos del fabricante, o con desarrollos personalizados ejecutados por Operbes S.A. de C.V. .
- Capacidad para almacenar la información tal y como fue recibida del dispositivo o aplicaciones (eventos en crudo), para efectos de auditoría y análisis forense. La solución generará una firma o "checksum" de los eventos recibidos para garantizar la integridad y mantendrá la cadena de custodia.
- Permitirá la detección automática de fuentes de eventos recolectados a través del protocolo syslog, el cual puede ser enviado vía UDP, TCP o SSL/TLS.
- Capacidad de permitir filtrar eventos por cualquier campo del registro, que son los atributos donde se almacena la información recolectada por la herramienta de las fuentes de eventos.
- Contará con lógica de taxonomía a nivel de la recolección de los eventos, y que permita definir y modificar la misma con base en los eventos auditados.
- Capacidad para detectar automáticamente la desconexión de un conector de integración a través del envío de señales de comunicación para el aseguramiento de la continuidad operativa ("Keep Alive").
- Capacidad para integrarse con los sistemas de detección y prevención de intrusos y los de administración de vulnerabilidades (VM)
- Contará con la capacidad de emitir notificaciones a partir de eventos y datos recopilados a través de mecanismos como SMTP, SNMP y SYSLOG.
- Correlacionará eventos en tiempo real, es decir, que la información de los eventos sobre los que se está basando deberá venir del flujo del bus de mensajes.
- Capacidad para definir reglas de correlación con distintos niveles de complejidad, partiendo de las basadas en patrones, hasta reglas basadas en periodos de tiempo, anidadas, causa/efecto y secuenciales.
- El módulo de creación de reglas de correlación deberá tener la capacidad de seleccionar eventos para hacer las reglas, así como el seleccionar campos del mismo para ser incluidos en la regla a través de mecanismos como "Drag-and-Drop".



ANEXOS
DIVISIÓN DE CONTRATOS

- Contará con la capacidad de probar las reglas antes de ser implementadas en el motor de correlación.
- Comprimirá los datos almacenados al menos con una relación de 10 a 1.
- Contará con mecanismos de monitoreo de la integridad de la información local y archivada.
- Capacidad para soportar de forma nativa la integración con soluciones de almacenamiento en red como SAN, NAS, NFS o CIFS.
- Contará con una suscripción de boletines de seguridad más importantes del mercado para así identificará las vulnerabilidades conocidas, correlacionando la información de herramientas de administración de vulnerabilidades con los eventos recolectados, lo que permitirá automatizar su detección.

**12. Servicio de Protección de Amenazas Persistentes Avanzadas (APT)**

Operbes S.A. de C.V. proporcionará mínimo 2 y máximo 4 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuraciones en HA)

Operbes S.A. de C.V. tomó en consideración que se acepta que la solución de HA se establezca a través de 2 cajas activas mediante una sola IP virtual.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 256 de la empresa Global Boga, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que se requiere inspeccionar al menos 100,000 archivos por día.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 257 de la empresa Global Boga, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que en este tipo de servicios las cajas pueden funcionar de manera activa a través de balanceador y acepta la convocante este método como propuesta para HA
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 271 de la empresa Nelson Morgan Consulting, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que la inspección por día de la solución será al menos 5 Gbps por segundos.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 272 de la empresa Nelson Morgan Consulting, S.A. de C.V. y pregunta 296 de la empresa Operbes, S.A. de C.V.

Especificaciones Técnicas:

- Detectará cuando un equipo intenta hacer comunicación con un servidor de comando y control en Internet.
- Detectará cuando una amenaza intenta ingresar en la organización mediante internet.
- Detectará e interactuar cuando un atacante o código maliciosos está realizando actividades de movimientos laterales en la organización.
- Detectará ataques del tipo "zero day" que puedan intentar comprometer activos de la organización.
- Tendrá las capacidades de detección de anomalías en los puntos de la red designados, dicha detección no debe basarse en firmas ni heurística.

- Tendrá la capacidad de actuar no solo por la generación de alertas de los componentes tecnológicos implementados, si no capacidades de caza de amenazas.
- Contará con las capacidades de análisis y perfilamiento de los actores detrás de un ataque sobre el Instituto.
- Apoyará al Instituto en la detección y prevención de ataques avanzados, así como el manejo de los incidentes que deriven de ello.
- Elevará el nivel de visibilidad respecto a detección de amenazas avanzadas persistentes.
- Elevará el nivel de capacidades de actuación ante una amenaza avanzada persistente.
- Permitirá contar con la información suficiente para identificar el impacto real de una amenaza.
- Permitirá proteger diversos segmentos de la red del Instituto con diferentes niveles de protección de acuerdo con la criticidad de los usuarios de cada segmento.
- Permitirá tener arquitectura modular y escalable de protección y viabilidad.
- Contará con un servicio especializado que permita apoyar al Instituto en la actuación y respuesta ante un ataque desarrollado con amenazas avanzadas.
- Acortará los tiempos de detección y actuación ante una amenaza avanzada.
- Integrará las capacidades de identificar una amenaza cuando tiene comunicación al exterior mediante el servicio de internet del Instituto o movimiento laterales en las diversas localidades, estas capacidades de detección tendrán la capacidad de perfilar el comportamiento de los usuarios y sus dispositivos con el propósito de detectar cualquier anomalía que puede representar un impacto o riesgo para la Institución
- Dispondrá de una capa de inteligencia provista por los fabricantes de los componentes tecnológicos y fortalecida por la capa de inteligencia propia de Operbes S.A. de C.V. ; dichas capas incluirán al menos las siguientes características:
  - IP, URL Maliciosos
  - Hashes de archivos maliciosos
  - Tácticas, técnicas y procedimientos de los atacantes de la región en organizaciones similares al Instituto.
- Proporcionará las capacidades de realizar investigaciones en profundidad para detectar intrusiones que han pasado desapercibidas para los controles de seguridad implementados, esta investigación permitirá al menos las siguientes capacidades:
  - Caza de amenazas que han estado activas, pero por su comportamiento no han podido ser detectadas.
  - Interacción con el código malicioso y ataques mediante la implementación de trampas en la red y la emulación de servicios.
  - Engaño de los atacantes mediante la implementación de información que pueda rastrear el origen de un ataque.
  - Análisis dinámico de los artefactos detectados.
  - Análisis de indicadores de compromiso en la red de cómputo del Instituto.
- Generará inteligencia accionable con la cual se puedan alimentar los controles preventivos para evitar que una amenaza conocida pueda volver a presentarse o la detección y contención sea temprana.

## 13. Antivirus

Operbes S.A. de C.V. proporcionará servicios para el centro de datos principal ubicado en Morelia Michoacán en HA

Operbes S.A. de C.V. tomó en consideración que la solución podrá desplegarse en nube en un esquema SaaS con lo cual la alta disponibilidad está garantizada con las mejores condiciones para EL INSTITUTO.



ANEXOS
DIVISIÓN DE CONTRATOS

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 579 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que los equipos a que se refiere a las consolas antivirus requeridos para Morelia, Michoacán y estas serán desplegadas en nube en esquema SAAS según lo indica en la respuesta otorgada en la pregunta 579.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 31 de la empresa Operbes, S.A. de C.V.

Especificaciones Técnicas:

La solución propuesta por Operbes S.A. de C.V. contará con las siguientes funcionalidades:

- La solución antivirus protegerá a los siguientes sistemas operativos, en las plataformas Intel y AMD (Windows Server 2012 y posteriores).
- La solución antivirus integrará agentes para la detección de virus, malware, entre otros en las plataformas de correo electrónico institucional (Exchange Server 2010 y superiores)
- Reputación Web
  - La solución de antivirus contará con un sistema basado en la reputación de sitios web que permitan de manera proactiva evitar que los usuarios cuando naveguen descarguen componentes maliciosos e infecten sus estaciones de trabajo.
  - El sistema de reputación de archivos estará integrado o desagregado de la consola de antimalware.
  - Niveles de seguridad para evitar la navegación Web a sitios maliciosos cuando los usuarios se encuentran dentro o fuera de la red corporativa.
  - Permitirá reclasificar sitios web.
  - El sistema de protección Web no dependerá de ningún explorador en específico.
  - Permitirá editar la lista de URL permitidas a nivel general, grupos o personal.
- Ataques de día Zero
  - Cuando es publicada o descubierta una vulnerabilidad en sistema operativo o en alguna aplicación, el Antimalware será capaz de detener un ataque causado por un malware que aprovecha la vulnerabilidad descubierta.
- Protección Antimalware
  - Detectará, analizará y eliminará programas maliciosos, como virus, spyware, gusanos, troyanos, keyloggers, programas publicitarios, rootkits, phishing, entre otros.
  - Detectará, analizará y eliminará, de forma automática y en tiempo real, los programas maliciosos en:
    - Procesos que se ejecutan en la memoria principal (RAM);
    - Archivos creados, copiar, renombrar, mover o modificados, incluyendo períodos de sesiones en la línea de comandos (DOS o shell) abiertos por el usuario;
    - Archivos comprimidos de forma automática, al menos en los siguientes formatos: ZIP, EXE, ARJ, MIME / UU, CAB de Microsoft, Microsoft Comprimir.
    - Archivos recibidos a través de software de comunicación instantánea (Whatsapp, MSN Messenger, Yahoo Messenger, Google Talk, ICQ, entre otros).
  - Detectará y protegerá a la estación de trabajo contra acciones maliciosas que se ejecutan en navegadores Web mediante secuencias de comandos en lenguajes tales como JavaScript, VBScript / ActiveX, etc.
  - La detección heurística de virus desconocidos.
- Control de dispositivos
  - Proporcionará o restringirá el acceso a dispositivos USB, Floppy, CD´s y Carpetas compartidas.

- La solución Antimalware evitará una infección provocada por la ejecución del archivo Autorun.inf contenido en un dispositivo de USB al momento de ser conectado en la estación de trabajo.
- Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware permitirá al usuario hacer modificaciones, control total, solo lectura y ejecución, solo lectura en el contenido del dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger.

- Protección por comportamiento
  - Para aquellos programas que no están permitidos ser ejecutados en la estación de trabajo, serán agregados a una lista de bloqueo de programas específicos.
  - Evitará o monitoreará que un programa con comportamiento sospechoso pueda realizar lo siguiente:
    - Duplicará o inyectará archivos de sistema similares.
    - Modificará el archivo de HOST.
    - Incrustará elementos "plugins" en el navegador de Internet Explorer.
    - Instalará librería del programa malicioso.
    - Instalará nuevos servicios.
    - Modificará archivos de sistema.
    - Instalará servicios o programas para iniciarse al arrancar la estación de trabajo.
- Reporte de amenazas a los laboratorios
  - Capacidad de reportar eventos de amenazas aún no identificadas, de manera automática a través del comportamiento, a los laboratorios de antimalware para el análisis e identificación de la fuente y generación de una protección proactiva.
  - Capacidad de limitar los recursos utilizados para la notificación a los laboratorios, respetando la confidencialidad de la información.
  - Lanzará una política de seguridad en caso de epidemias.
- Métodos de Actualización, Instalación y desinstalación
  - Instalación de cliente antivirus mediante la URL de la Consola de la solución.
  - Instalación de cliente antivirus mediante línea de comandos o script.
  - Lanzamiento de instalación vía navegación de los grupos de trabajo de Windows.
  - Lanzamiento de instalación vía integración con el dominio de Active Directory.
  - Lanzamiento de instalación vía escaneo de equipos dentro de un segmento de Red.
  - Desinstalación del cliente desde el administrador de programas de Windows o el acceso directo a Uninstall.exe del menú inicio.
  - Desinstalación del cliente de forma remota desde la consola de administración.
  - Configuración de Actualizaciones automáticas, así como la fuente de actualización.
  - Distribución de actualizaciones a los clientes de manera Automática y Manual.
  - Actualización de sistema de firmas para clientes sin conectividad al servidor.
  - Actualización de grupo de usuarios por Agentes de Actualización o repositorios.
- Configuración de escaneos
  - Personalización de opciones de escaneo y Acción para una detección en los modos: Manual, en Tiempo Real y Programado.
- Privilegios de los usuarios
  - Personalizará los permisos de los clientes para realizar acciones en el software local.
  - Inhabilitación de los servicios y/o componentes del Cliente antivirus por medio de contraseña.
  - Habilitará o deshabilitará opciones para el cliente que frecuentemente entra/sale de la red local.

## 14. Servicios propuestos de Prevención de Perdida de Información

Operbes S.A. de C.V. incluye como alcance de la presente propuesta estos servicios para el centro de datos principal ubicado en Morelia Michoacán en HA

Operbes S.A. de C.V. tomó en consideración que la solución requerida implica la provisión de appliances de propósito específico para cumplir con las funcionalidades requeridas.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 298 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que los applices de propósito especifico se refiere a las consolas de gestión de los agentes de Prevención de Perdida de Información requeridos para Morelia, Michoacán.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 16 de la empresa Operbes, S.A. de C.V.

Especificaciones Técnicas propuestas:

La solución propuesta por Operbes S.A. de C.V. cuenta con las siguientes funcionalidades:

- Presentar un Log de auditoría de todas las actividades de los usuarios.
- Proporcionar Reportes predefinidos y personalizados que puedan ser programados o de una sola vez.
- Proporcionar un mecanismo de alertas y notificaciones.
- Es capaz de proporcionar administración basada en roles múltiples con las siguientes opciones:
  - Capacidad para definir roles de usuarios tales como Administrador, administrador de la seguridad o administrador de cuentas.
  - Capacidad para agregar y modificar roles personalizados.
  - Capacidad de configurar cuentas de usuario y asignar un rol particular a cada usuario.
- Tecnología de Detección.
  - Capacidad para extraer textos de diferentes tipos de documentos para ejecutar escaneos de contenido.
  - Capacidad de realizar detecciones basadas en palabras (keywords) personalizadas o frases (key phrases) personalizadas, con la habilidad de poner diferentes palabras en una sola regla de detección.
  - Capacidad de detección basada en expresiones regulares.
  - Capacidad de detección basada en atributos de archivos tales como tipo de archivo y tamaño de archivo.
  - Capacidad de utilizar validación de reglas de expresión.
  - Capaz de extraer y ejecutar escaneo de contenido de documentos dentro de archivos comprimidos tales como archivos zip y rar.
  - Capaz de controlar la cantidad de capas de compresión que va a descomprimir en archivos comprimidos.
  - Capaz de soportar texto en diferentes idiomas (al menos español e inglés).
  - Que sea capaz de definir identificadores de datos a través de palabras, expresiones o atributos de archivos.
  - Proporcione identificadores de datos predefinidos.
  - Capaz de duplicar y personalizar identificadores de datos predefinidos y personalizados.
  - Capaz de crear identificadores de datos múltiples.
  - Que sea capaz de combinar palabras, expresiones y atributos de archivos dentro de plantillas para identificar información sensible.
  - Proporcione plantillas predefinidas.
  - Con capacidad para importar y exportar plantillas.
  - Capacidad para crear diversas plantillas personalizadas.

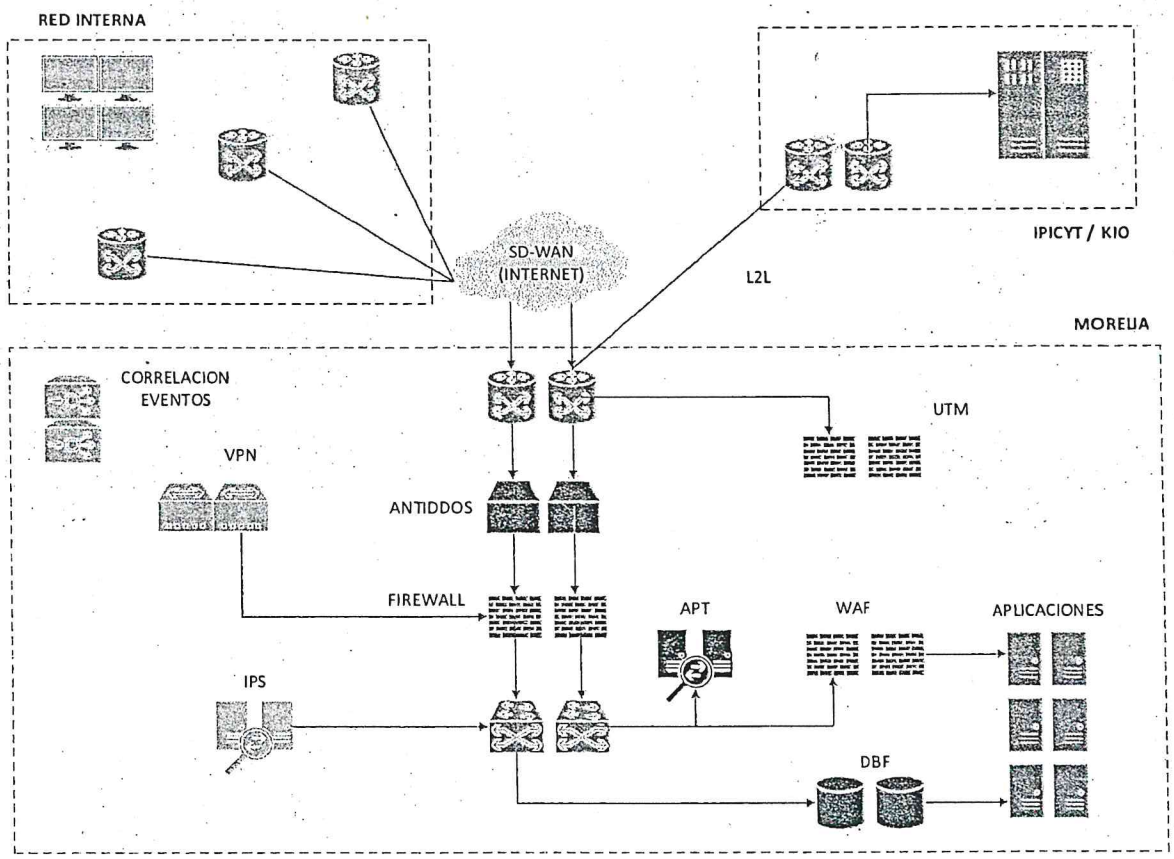
- Capaz de combinar diversas plantillas dentro de una política.
- Capacidad de crear diversas políticas.
- Capacidad de crear políticas desde la consola de administración centralizada.
- Capaz de soportar diversas acciones para una política simple.
- Capaz de definir un set diferente de acciones basado en la condición de la máquina si está dentro o fuera de la red.
- Capaz de soportar las siguientes acciones cuando haya fuga de información sensible:
  - Sólo registro del evento (Log violation only).
  - Bloqueo de la transferencia de datos (Block data transfer).
  - Alertas en el equipo del cliente (Client-side alerts).
  - Alertas en el servidor de DLP (Server-side alerting).
  - Almacenamiento de información para análisis forense (Forensic data-capture)

- Es capaz de ejecutar escaneos de contenido en los siguientes canales de información:
  - Correo electrónico
  - HTTP/HTTPS
  - FTP
  - Dispositivos removibles
  - Copia de información a CD/DVD
  - Mensajería instantánea
  - Comando de impresión
  - P2P
  - Portapapeles
  - Correo web
- Es capaz de restringir acceso a los siguientes dispositivos:
  - Unidades extraíbles
  - Unidades ópticas
  - IEEE 1394
  - Impresión de pantalla
  - Bluetooth
  - Tarjetas PCMCIA
  - Carpetas compartidas
- Es capaz de especificar excepciones de dispositivos
  - Capaz de definir diversas excepciones.
  - Capaz de utilizar comodines cuando se defina una excepción de dispositivos.
  - La configuración de control de dispositivos se debe de realizar de forma centralizada, desde la consola de administración.
  - Capaz de enviar un mensaje de notificación en la computadora del cliente.
  - Capaz de guardar en el log los eventos de control de dispositivos.

**15. Generales para todas las soluciones propuestas**

- Todas las soluciones cumplen como mínimo con estas especificaciones y capacidades, lo cual son enunciativas más no limitativas.
- La presente propuesta considera todos los componentes necesarios para su correcta operación (Equipo activo de Telecomunicaciones, cableado, módulos, etc.)
- La presente propuesta técnicas, se acompaña de las hojas de especificaciones, trípticos y demás información que permite verificar el cumplimiento de las mismas.
- Operbes S.A. de C.V. tomó en consideración que puede realizar propuestas de mejora de cada una de las soluciones y/o diseño de la red con forme a sus propuestas. (Ver el diagrama 01 propuesta de las soluciones).
- Operbes S.A. de C.V. tomó en consideración que puede proponer arreglos tipo cluster.

DIAGRAMA 01. PROPUESTA DE LAS SOLUCIONES




**16. Especificaciones físicas y estándares propuestas de conexión para los insumos que conforman los Servicios Administrados de Seguridad Informática 2022-2024**

- Propuesta de especificaciones de energía eléctrica

Operbes S.A. de C.V. tomó en consideración que el Instituto proporcionará las facilidades dentro de los centro de datos para la alimentación eléctrica (contactos regulados), para el funcionamiento y operación del equipamiento propuesto, Operbes S.A. de C.V. considera como alcance de la presente propuesta técnica las características, cantidad, ubicación y los tipos de contactos requeridos para el aprovisionamiento inicial. Para dar cumplimiento con este punto favor de referirse al documento llamado "Especificaciones técnicas de los equipos propuestos" dentro de la presente propuesta técnica.

- Especificaciónes propuestas de espacio físico y ambiental

Operbes S.A. de C.V. tomó en consideración que el Instituto proporcionará la información específica respecto al espacio físico asignado para que Operbes S.A. de C.V. en caso de resultar adjudicado, instale la infraestructura de redes y seguridad en los centro de datos correspondientes. Para tal efecto Operbes S.A. de C.V. incluye en la presente propuesta técnica un apartado indicando la cantidad de espacio físico mínimo indispensable que se requerirá para la instalación de la infraestructura de seguridad. Para dar

cumplimiento con este punto favor de referirse al documento llamado "Especificaciones técnicas de los equipos propuestos" dentro de la presente propuesta técnica.

También se deberá contar con las facilidades para su instalación y Operbes S.A. de C.V. se apegará al reglamento y políticas internas para la instalación dentro de cada Centro de Datos. Así también se indican las condiciones ambientales adecuadas para el funcionamiento del equipo a instalar para dar el servicio. Para dar cumplimiento con este punto favor de referirse al documento llamado "Especificaciones técnicas de los equipos propuestos" dentro de la presente propuesta técnica.

- Especificaciónes propuestas para el montaje de hardware

Debido a que el requerimiento del Instituto es un servicio administrado, será responsabilidad de Operbes S.A. de C.V. , el montaje de los equipos propuestos, racks, gabinetes, rack de panel de parcheo (Parch panel rack), distribuidores fibra óptica, y todo lo necesario para la correcta operación de la solución propuesta, por lo que, en su propuesta económica se considera todo lo necesario con la finalidad de proveer lo necesario.

- Especificación propuesta para racks

Operbes S.A. de C.V. en caso de resultar adjudicado cumplirá las especificaciones de los racks y gabinetes, incluyendo sus dimensiones físicas, para cada uno de los centros de datos donde el Instituto indique para implementar los Servicios SASI 2022-2024, y en apego a las normas y estándares de la industria y los que se acuerdan o indiquen durante las mesas de trabajo con el Instituto.

Operbes S.A. de C.V. tomó en consideración que la cantidad y características técnicas de los racks y gabinetes depende de los activos de infraestructura que se implementen como parte del servicio.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 346 de la empresa Operbes, S.A. de C.V.

- Políticas propuestas de cableado estructurado en centro de datos

Operbes S.A. de C.V. en caso de resultar adjudicado cumplirá los requerimientos para cada uno de los Centros de Datos donde el Instituto indique implementar los Servicios SASI 2022-2024, y en apego a las normas y estándares de la industria y los que se acuerdan o indiquen durante las mesas de trabajo con el Instituto, así mismo Operbes S.A. de C.V. en caso de resultar adjudicado suministrará los elementos para la interconectividad necesarios, por lo que proporcionará e implementar los distribuidores de fibras, las canaletas, los jumpers, y cualquier otro elemento que sea necesario para la correcta interconexión de los racks o puntos de interconexión bajo los estándares de cableado estructurado.

Operbes S.A. de C.V. tomó en consideración que las características técnicas del cableado estructurado son: Fibra óptica Multimodo de OM1 al OM5, Cable UTP Categoría 5E o superior, dependiendo de cantidad de activos de infraestructura que se implemente como parte del servicio.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 347 de la empresa Operbes, S.A. de C.V.

- Especificación propuesta de cableado para racks

Operbes S.A. de C.V. considera como alcance de la presente propuesta (tanto para el aprovisionamiento inicial, como durante la operación y vigencia del contrato), todo el cableado, jumpers y patch cords necesarios para lograr la interconexión propuesta de todos y cada uno de los módulos y elementos del sistema propuesto.

- Especificaciones y requerimientos técnicos de cableado y conectores

Todos los componentes del sistema de cableado, así como troncales de cobre y/o fibra –excepto los correspondientes a los servidores- necesarios para la interconexión de todos los módulos de hardware solicitados para suministrar el servicio de SASI 2022-2024 en el Centro de Datos deberán incluirse como parte de la propuesta de los Licitantes y deberán ser sin costo extra para el IMSS. Asimismo, en el caso de incrementos en los servicios deberán estar incluidos.

- Especificaciones y requerimientos técnicos propuestos para equipo de comunicaciones de red

Todos los componentes de interconexión (comunicaciones o balanceo de cargas) que apoyen la operación y administración que se lleve a cabo entre las soluciones de seguridad y red, que por su naturaleza sean propuestos para la puesta en operación del servicio de SASI 2022-2024 en el Centro de Datos, se incluyen como parte de la presente propuesta sin costo extra para el IMSS. Asimismo, en el caso de incrementos en los servicios estarán incluidos.

- Políticas de seguridad propuestas para acceso físico a externos

Operbes S.A. de C.V. cumplirá las políticas de seguridad de acceso físico a externos en los centros de datos donde el instituto determine para la provisión de los Servicios correspondientes SASI 2022-2024.

- Especificación y requerimientos propuestos para el sistema de canalización.

Operbes S.A. de C.V. en caso de resultar adjudicado salvaguardará la integridad física del cableado para evitar fallas potenciales en la operación. De este modo, para salvaguardar la correcta operación del sistema de cableado de fibra óptica y cableado UTP, Operbes S.A. de C.V. en caso de resultar adjudicado utilizará la infraestructura existente en los Centros de Datos y, en general, cumplirá con las norma y políticas de canalización en los mencionados Centros de Datos.

**17. Condiciones propuestas para los servicios de mantenimiento**

Operbes S.A. de C.V. en caso de resultar adjudicado será responsable de realizar las tareas de mantenimiento preventivo y correctivo para la totalidad de la infraestructura dentro del alcance de los servicios de SASI 2022-2024, a través de las labores que considere necesarias y de acuerdo con la estrategia de entrega y soporte de los servicios correspondientes. Enseguida se detallan las condiciones específicas para este servicio.

**18. Condiciones propuestas para los servicios de mantenimiento preventivo**

Como parte del Servicio de Mantenimiento, Operbes S.A. de C.V. en caso de resultar adjudicado realizará al menos un mantenimiento preventivo al año a toda la infraestructura que forme parte del contrato de SASI 2022-2024. Para lo cual integra un Plan de Mantenimiento Preventivo, en el cual tomará en cuenta para la proyección de mantenimientos, las ventanas de mantenimiento necesarias, con el fin de ser programadas e informadas con anticipación al administrador del contrato, con objeto de minimizar el impacto a la operación.

En la correspondiente propuesta técnica Operbes S.A. de C.V. incluye un Plan de Mantenimiento Preventivo, el cual incluye como mínimo:

- La descripción de los procesos asociados.
- Los Recursos Humanos y Materiales involucrados.
- Los alcances técnicos del mantenimiento y los protocolos de prueba.
- Las rutas de escalamiento correspondientes.

Para dar cumplimiento con este punto favor de referirse al documento llamado "Plan de Mantenimiento Preventivo y Correctivo para los servicios de seguridad" dentro de la presente propuesta técnica.

Esta información se agrupa por tipo de equipo o infraestructura. Para cada caso, Operbes S.A. de C.V. en caso de resultar adjudicado contemplará el calendario de los servicios de mantenimiento preventivo, el cual será validado y autorizado por administrador del contrato, quien revisará que no afecte períodos críticos de la operación del Instituto.

Operbes S.A. de C.V. tomó en consideración que el calendario final de mantenimientos preventivos, fundamentado en el Plan de Mantenimiento Preventivo que se entregará durante las Mesas de Trabajo, será elaborado por Operbes S.A. de C.V. en caso de resultar adjudicado y autorizado por el Instituto, acotando los inmuebles, fechas y actividades a realizar con el máximo detalle, a efectos de coordinar todas las labores necesarias para su correcta ejecución.

**19. Condiciones propuestas para los servicios de mantenimiento correctivo**

Operbes S.A. de C.V. en caso de resultar adjudicado será responsable de realizar el mantenimiento correctivo para los servicios correspondientes de SASI 2021-2024, para lo cual, previamente integra en la presente propuesta los procedimientos para reportar un incidente que requiera mantenimiento correctivo, y un ejemplo de matriz de escalamiento con los niveles y tiempos establecidos entre cada nivel.
Para dar cumplimiento con este punto favor de referirse al documento llamado "Plan de Mantenimiento Preventivo y Correctivo para los servicios de seguridad" dentro de la presente propuesta técnica.

Operbes S.A. de C.V. tomó en consideración que como parte de las Mesas de Trabajo, Operbes S.A. de C.V. proporcionará la Matriz de Escalamiento con los nombres de contactos y responsables.

Operbes S.A. de C.V. efectuará el servicio de Mantenimiento Correctivo cuantas veces sea necesario durante la vigencia del servicio, de acuerdo con las especificaciones técnicas del fabricante y consistirá en la reparación o remplazo de las partes dañadas del equipo, cuando ocurra una falla que así lo requiera.

Si el equipo en cuestión no puede ser reparado, se sustituirá por otro equipo de características técnicas iguales o superiores, sin que esto implique la degradación del nivel de servicio requerido para dicho equipo. El tiempo para el reemplazo de partes no excederá los 30 días naturales, durante los cuales Operbes S.A. de C.V. proporcionará un equipo provisional para mantener la operación. El tiempo para el reemplazo de equipos no excederá los 45 días naturales, durante los cuales Operbes S.A. de C.V. proporcionará un equipo provisional para mantener la operación.

ANEXOS
DIVISIÓN DE CONTRATOS

# Apéndice "B"

## Servicios Administrados de Seguridad Informática propuestos (SASI) 2022-2024

**Objetivo del Documento**

Presentar un documento que contiene los alances y las especificaciones técnicas y de calidad.

**2. Inventario de Activos de Infraestructura – Servicios de Continuidad**

Operbes S.A. de C.V. tomó en consideración el siguiente inventario:

| CONCEPTO | Sitio | Marca | Modelo | Número Serie |
|---|---|---|---|---|
| **I. Servicios de Seguridad - Continuidad Operativa** | | | | |
| 1. Arquitectura de Firewall. | | | | |
| Tipo 1 | IPICYT | Fortinet | FG-1100E | FG10E0TB21900070 |
| Tipo 2 | CENATI MONTERREY | Fortinet | FG-1100E | FG10E0TB21900374 |
| | CENATI MONTERREY | Fortinet | FG-1100E | FG10E0TB20903342 |
| Tipo 3 | CENATI MÉXICO | Fortinet | FG-1800F | FG180FTK20900846 |
| | CENATI MÉXICO | Fortinet | FG-1800F | FG180FTK20901096 |
| | JALISCO | Fortinet | FG-1800F | FG180FTK20900666 |
| | JALISCO | Fortinet | FG-1800F | FG180FTK20900667 |
| Tipo 4 | IPICYT | Fortinet | FG-4200F | FG420FTK20900121 |
| | IPICYT | Fortinet | FG-4200F | FG420FTK20900136 |
| 2. Prevención de Intrusiones (IPS) | | | | |
| Tipo 1 | CENATI MÉXICO | Fortinet | FG-1800F-BDL-950-12 | FG180FTK20901206 |
| Tipo 2 | CENATI MONTERREY | Fortinet | FG-2200E-BDL-950-12 | FG2K2ET920900397 |
| Tipo 3 | CENATI MÉXICO | Fortinet | FG-3300E-BDL-950-12 | FG3K3ET919900293 |
| | CENATI MÉXICO | Fortinet | FG-3300E-BDL-950-12 | FG3K3ET919900310 |
| Tipo 4 | IPICYT | Fortinet | FG-3300E-BDL-950-12 | FG3K3ET919900331 |
| | IPICYT | Fortinet | FG-3300E-BDL-950-12 | FG3K3ET919900323 |
| 3. Anti-denegación de servicios DDoS | | | | |
| Tipo 1 | CENATI MONTERREY | Fortinet | FDD-1500F | FI1K5FTE20000010 |
| | CENATI MONTERREY | Fortinet | FDD-1500F | FI1K5FTE20000039 |
| Tipo 2 | IPICYT | Fortinet | FDD-1500F | FI1K5FTE20000009 |
| | IPICYT | Fortinet | FDD-1500F | FI1K5FTE20000045 |
| 4. Redes Privadas Virtuales (VPN) | | | | |
| | IPICYT | Fortinet | FG-1100E | FG10E0TB21900305 |

| | | | | |
|---|---|---|---|---|
| | IPICYT | Fortinet | FG-1100E | FG10E0TB20903417 |
| | IPICYT | Fortinet | FG-1100E | FG10E0TB20903544 |
| | IPICYT | Fortinet | FG-1100E | FG10E0TB21900273 |
| 5. Filtrado de contenido web (WEBFILTERING) | | | | |
| | IPICYT | Fortinet | FG-1801F-BDL-950-12 | FG181FTK20900649 |
| | IPICYT | Fortinet | FG-1801F-BDL-950-12 | FG181FTK20900909 |
| | IPICYT | Fortinet | FG-1801F-BDL-950-12 | FG181FTK20901026 |
| | IPICYT | Fortinet | FG-1801F-BDL-950-12 | FG181FTK20901059 |
| 6. Antispam | | | | |
| | IPICYT | Fortinet | FML-3200E-BDL-641-12 | FE3K2ET319000024 |
| | IPICYT | Fortinet | FML-3200E-BDL-641-12 | FE3K2ET319000028 |
| | IPICYT | Fortinet | FML-3200E-BDL-641-12 | FE3K2ET319000029 |
| | IPICYT | Fortinet | FML-3200E-BDL-641-12 | FE3K2ET319000035 |
| 7. Firewall Especializado en Servicios Web (WAF) | | | | |
| | IPICYT | IMPERVA | X10K2 | 2030BA3322 |
| | IPICYT | IMPERVA | X10K2 | 2030BA3319 |
| | CENATI MONTERREY | IMPERVA | X10K2 | 2030BA4461 |
| | CENATI MONTERREY | IMPERVA | X10K2 | 2030BA4457 |
| 8. Firewall de Base de Datos (DBF) | | | | |
| | IPICYT | IMPERVA | X6520 | 2030BA3391 |
| | IPICYT | IMPERVA | X6520 | 2030BA3392 |
| | CENATI MONTERREY | IMPERVA | X6520 | 2113BA0235 |
| | CENATI MONTERREY | IMPERVA | X6520 | 2113BA0238 |
| 9. Gestión Unificada de Amenazas (UTM) | | | | |
| Tipo 1 | ATLIXCO | Fortinet | FG-100F-BDL-950-12 | FG100FTK21003654 |
| Tipo 2 | OAXTEPEC | Fortinet | FG-400E-BDL-950-12 | FG4H0ETB20902009 |
| Tipo 3 | CENATI MONTERREY | Fortinet | FG-600E-BDL-950-12 | FG6H0ETB21901099 |
| Tipo 4 | CENATI MÉXICO | Fortinet | FG-1800F-BDL-950-12 | FG180FTK20901163 |

Operbes S.A. de C.V. tomó en consideración que se cuenta con los appliances de gestión y reporteo de las siguientes soluciones mencionadas en la tabla:

1. Arquitectura de Firewall.
2. Prevención de Intrusiones (IPS)

3. Anti-denegación de servicios DDoS
4. Redes Privadas Virtuales (VPN)
5. Filtrado de contenido web (WEBFILTERING)
6. Antispam
9. Gestión Unificada de Amenazas (UTM)
7. Firewall Especializado en Servicios Web (WAF)
8. Firewall de Base de Datos (DBF)

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, preguntas 301 y 302 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que las plataformas o consolas de gestión forman parte de los activos de infraestructura que el Instituto tiene operando actualmente y las cuales estarán disponibles al momento del proceso de transición.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 552 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que dichas plataformas o consolas de gestión pueden ser utilizadas por el PROVEEDOR adjudicado para proporcionar el servicio conforme a su estrategia.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 553 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que el Licitante adjudicado proporcionará el licenciamiento para la
continuidad operativa de los servicios, sin importar la vigencia de término del mismo.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 554 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que son propiedad del Instituto Mexicano del Seguro Social, de todos y cada uno de los equipos indicados en el "2. Inventario de Activos de Infraestructura – Servicios de Continuidad del Apéndice "B""
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 555 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración el inventario de las consolas de administración y reporteo con las cuales actualmente administran el inventario del apéndice B y son las siguientes:

| Ubicacion | Marca | Tecnologia | Modelo | Equipo | Numero de serie | Version de Firmware |
|---|---|---|---|---|---|---|
| CENATI MTY | Imperva | WAF | X8170 | IMSSCENATIMTYWAF-MX | 211D8A41BB | 14.1.0.15_0 |
| IPICYT SLP | Imperva | WAF | X8170 | IMSSIPICYTWAF-MX | 201BA341L5 | 14.1.0.15_0 |
| IPICYT SLP | Fortinet | FortiManager | FMG-2000E | IMSSIPICYTFMG-2000E | FMG2KE1320000084 | v6.4.7-build2412 210902 |
| IPICYT SLP | Fortinet | FortiAnalyzer | FAZ-3000G | IMSSIPICYTFAZ-3000G | FAZ3KGT2200000084 | v6.4.7-build2412 210902 |
| IPICYT SLP | Fortinet | FortiAnalyzer | FAZ-3100G | IMSSIPICYTFAZCLL1-3000G | FAZ3KGT2200000088 | v6.4.7-build2412 210902 |
| IPICYT SLP | Fortinet | FortiAnalyzer | FAZ-3100G | IMSSIPICYTFAZCLL2-3000G | FAZ3KGT2200000064 | v6.4.7 build2412 210902 |
| IPICYT SLP | Fortinet | FortiAnalyzer | FAZ-3100G | IMSSIPICYTFAZCLL-3000G | FAZ3KGT2200000033 | v6.4.7-build2412 210902 |

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 25 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que la infraestructura por renovar es propiedad del Instituto Mexicano del Seguro Social, por lo que existe la viabilidad por parte de los fabricantes de otorgar a quien lo requiera los derechos de uso del licenciamiento.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 42 de la empresa Axtel, S.A.B. de C.V.

## Apéndice "B-bis"

## Servicios Administrados de Seguridad Informática propuestos (SASI) 2022-2024

### 1. Objetivo del Documento

Operbes S.A. de C.V. tomó en consideración que el objetivo es presentar un documento que contiene los alances y las especificaciones técnicas y de calidad.

### 2. Inventario de Activos de Infraestructura – Servicios de Continuidad

Operbes S.A. de C.V. tomó en consideración como alcance de la presente propuesta los siguientes:

| No. | Descripción del servicio | Unidad de medida | Cantidad referencial mínima | Cantidad referencial máxima |
|---|---|---|---|---|
| 1 | Licenciamiento Firewall (Tipo 1) - Renovación | Servicio | 1 | 1 |
| 2 | Licenciamiento Firewall (Tipo 2) - Renovación | Servicio | 2 | 2 |
| 3 | Licenciamiento Firewall (Tipo 3) - Renovación | Servicio | 4 | 4 |
| 4 | Licenciamiento Firewall (Tipo 4) - Renovación | Servicio | 2 | 2 |
| 5 | Licenciamiento IPS (Tipo 1) - Renovación | Servicio | 1 | 1 |
| 6 | Licenciamiento IPS (Tipo 2) - Renovación | Servicio | 1 | 1 |
| 7 | Licenciamiento IPS (Tipo 3) - Renovación | Servicio | 2 | 2 |
| 8 | Licenciamiento IPS (Tipo 4) - Renovación | Servicio | 2 | 2 |
| 9 | Licenciamiento Anti-denegación de servicios DDoS (Tipo 1) - Renovación | Servicio | 2 | 2 |
| 10 | Licenciamiento Anti-denegación de servicios DDoS (Tipo 2) - Renovación | Servicio | 2 | 2 |
| 11 | Licenciamiento Redes Privadas Virtuales - Renovación | Servicio | 4 | 4 |
| 12 | Licenciamiento Filtrado de Contenido Web - Renovación | Servicio | 4 | 4 |
| 13 | Licenciamiento Filtrado de Contenido de Correo (Antispam) - Renovación | Servicio | 4 | 4 |
| 14 | Licenciamiento Firewall Especializado en Servicios Web (WAF) - Renovación | Servicio | 4 | 4 |
| 15 | Licenciamiento Firewall Especializado en Base de Datos (DBF) - Renovación | Servicio | 4 | 4 |
| 16 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 1) - Renovación | Servicio | 1 | 1 |



ANEXOS
DIVISIÓN DE CONTRATOS

| | | | | |
|---|---|---|---|---|
| 17 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 2) - Renovación | Servicio | 1 | 1 |
| 18 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 3) - Renovación | Servicio | 1 | 1 |
| 19 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 4) - Renovación | Servicio | 1 | 1 |

## Anexo 2.- Términos y Condiciones

### 1. Objetivo del documento

Presentar los alcances y condiciones de entrega de los "Servicios Administrados de Seguridad Informática 2022-2024" propuestos.

### 2. Premisa

Operbes S.A. de C.V. tomó en consideración que las bases de datos, aplicaciones y cualquier otro tipo de información utilizadas en el suministro de los servicios o a la que se tenga acceso derivado de la naturaleza de los servicios, que sean propiedad exclusiva del Instituto Mexicano del Seguro Social ("El Instituto") continuarán siendo propiedad exclusiva del mismo. En ese sentido, Operbes S.A. de C.V. se obliga a utilizarlas exclusivamente para cubrir los servicios propuestos.

Operbes S.A. de C.V. incluye como parte de la presente propuesta técnica, un escrito firmado por su representante legal respecto de las obligaciones de confidencialidad, las cuales estarán sujetas a lo dispuesto por la Ley Federal de Transparencia y Acceso a la Información Pública o por la Ley correlativa aplicable al Instituto. Para dar cumplimiento con este punto favor de referirse al documento llamado "Escrito firmado por su representante legal respecto de las obligaciones de confidencialidad" dentro de la presente propuesta técnica.

### 3. Nombre del proyecto

**"Servicios Administrados de Seguridad Informática 2022 – 2024"**

### 4. Objetivos del proyecto propuesto

Operbes S.A. de C.V. propone al Instituto Mexicano del Seguro Social (IMSS), a través de la Dirección de Innovación y Desarrollo Tecnológico (DIDT) el proporcionar de manera integrada y unificada, los servicios administrados que brinden la continuidad operativa, de negocio y de seguridad de la información del Instituto que:

- Asegure y proteger la información Institucional.
- Garantice la continuidad operativa, de negocio y de la seguridad de la información de la Institución, durante la vigencia del presente contrato, especialmente durante la toma de operación y transición del contrato anterior a los servicios propios de SASI 2022-2024.
- Fortalezca la seguridad de la información de la Institución contra amenazas, disminuyendo el riesgo de sufrir incidentes de seguridad, mediante el uso de tecnología de punta para el monitoreo, detección, aseguramiento, contención y respuesta ante ataques que puedan presentarse en la infraestructura de cómputo, sistemas y aplicaciones del IMSS.
- Cuente con servicios de infraestructura regulados por niveles de servicio, que: implementen (instalen, migren, habiliten y pongan a punto) los componentes necesarios en los centros de datos y servicios propios del IMSS y que de forma complementaria gestionen (operen, monitoreen, den soporte y mantenimiento preventivo y correctivo) a la correspondiente infraestructura con el propósito de satisfacer las necesidades de: conectividad, comunicación, protección, control y filtrado de la propia Institución, manteniendo la plataforma tecnológica en condiciones óptimas de operación.



ANEXOS
DIVISIÓN DE CONTRATOS

- Cuente con los servicios de protección de forma unificada e integrada, incluyendo prevención de pérdida de información, protección de cómputo físico o virtual, correo electrónico externo e interno, herramientas de colaboración, acceso a internet e intranet, filtrado; mediante una solución integral que permita una gestión consolidada de las funcionalidades, características y servicios, con el propósito de mantener, asegurar y robustecer el esquema de seguridad del IMSS.
- Cuente con servicios de seguridad de la información, que complementen el esquema de seguridad institucional de forma consistente y robusta, con el control, aseguramiento, diagnóstico, pruebas, metodologías, de distintos rubros como el de acceso a cuentas privilegiadas, base de datos, aplicaciones, fuentes múltiples, vulnerabilidades, investigación forense y de procesos de seguridad, así como con otros servicios especializados en materia de seguridad y tecnologías de la información.
- Cuente con servicios para la capacitación y de soporte extendido que tienen como objetivo coadyuvar en la prestación del resto de los servicios SASI 2022-2024.

**5. Normas oficiales o certificaciones propuestas**

- Certificado ISO/IEC27001:2013
- Certificado ISO/IEC20000-1:2018

Ambos se encuentran vigentes y a nombre de Operbes S.A. de C.V.

Para dar cumplimiento con este punto favor de referirse al documento llamado "certificados ISO/IEC27001:2013 e ISO/IEC20000-1:2018 vigentes" dentro de la presente propuesta técnica.

**6. Folletos, catálogos, fotografías, manuales entre otros**

Se incluyen de acuerdo a lo solicitado.

Operbes S.A. de C.V. tomó en consideración que los participantes en Partida 1 pueden proponer la sustitución de la infraestructura existente indicada en el Apéndice "B" Servicios Administrados de Seguridad Informática (SASI) 2022-2024 2. Inventario de Activos de Infraestructura – Servicios de Continuidad siempre que se cumplan con las características descritas en el Apéndice "A" y siempre y cuando cumpla con el alcance requerido por el Instituto.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 500 de la empresa Scitum, S.A. de C.V.

**7. Visitas a las instalaciones**

No se requiere por parte de la convocante.

**8. Tipo de abastecimiento requerido**

El tipo de abastecimiento será mediante lo considerado en la partida propuesta.

**9. Garantías**

Operbes S.A. de C.V. , se obliga a constituir en la forma y términos previstos por los artículos 48 y 49 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 103 de su Reglamento y numerales 4.30 y 4.30.3 de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social, la garantía de cumplimiento divisible correspondiente.

En cualquier momento, el instituto podrá hacer válida la póliza de garantía del contrato en caso de que Operbes S.A. de C.V. no cumpla con los tiempos y plazos de entrega establecidos en los presentes Términos y Condiciones.

Operbes S.A. de C.V. tomó en consideración que las modificaciones a las fianzas deberán formalizarse con la participación que corresponda a la afianzadora, en términos de las disposiciones aplicables.

Operbes S.A. de C.V. tomó en consideración que la garantía permanecerá vigente a partir de la fecha de adjudicación del contrato respectivo, y hasta que se cumplan plenamente todas y cada una de las obligaciones del contrato, así como durante la substanciación de todos los recursos legales o juicios que, en su caso, sean interpuestos por cualquiera de las partes y hasta que se dicte la resolución definitiva por autoridad competente.

Operbes S.A. de C.V. tomó en consideración que para garantizar el cumplimiento de todas y cada una de las obligaciones estipuladas en el contrato Adjudicado, se compromete a entregar, dentro de los 10 (diez) días naturales posteriores a la firma del contrato correspondiente, de conformidad con el artículo 103 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, por el 10% del monto máximo por el que se adjudica el contrato, a favor del instituto, el cual será un contrato abierto y la garantía será divisible.

Bestel, se obliga a entregar a el Instituto la póliza de fianza antes señalada, en la división de contratos, ubicada en calle Durango número 291, piso 10, Colonia Roma Norte, Alcaldía Cuauhtémoc, apegándose al formato que para tal efecto se entregará en la referida División.

**a) Devolución de garantías**

Operbes S.A. de C.V. tomó en consideración que la liberación de garantías relativas al cumplimiento del Contrato podrán realizarse una vez que haya transcurrido el plazo de garantía indicado, a solicitud expresa de Operbes S.A. de C.V. por escrito en papel membretado de su empresa, dicha solicitud se dirigirá a la Coordinación de Adquisición de Bienes y Contratación de Servicios, quien autorizará la devolución o cancelación de la póliza de garantía (fianza) correspondiente, dicha autorización se entregará a Bestel, siempre que demuestre haber cumplido con la totalidad de las obligaciones adquiridas por virtud del presente Contrato.

La garantía de cumplimiento a las obligaciones del contrato únicamente podrá ser liberada mediante autorización expresa y por escrito otorgado por la División de Seguridad Informática Física.

**b) Ejecución de la garantía**

Operbes S.A. de C.V. tomó en consideración que se hará efectiva la garantía relativa al cumplimiento del contrato cuando:

- Operbes S.A. de C.V. incumpla con cualquiera de las obligaciones establecidas en el contrato que se celebre.
- Se rescinda administrativamente el contrato.
- La ejecución de la garantía será con independencia de la aplicación de las penas convencionales que procedan y de la rescisión administrativa del contrato.
- La ejecución de la garantía de cumplimiento del contrato será proporcional al monto de las obligaciones incumplidas.
- Además de las sanciones anteriormente mencionadas, serán aplicables las que estipulen las disposiciones legales vigentes en la materia.

**10. Acuerdos de Niveles de Servicio propuestos**



ANEXOS
DIVISIÓN DE CONTRATOS

El objetivo de los niveles de servicio propuestos por Operbes S.A. de C.V. , consiste en proporcionar al Instituto un mecanismo que permita:

- Medir de forma efectiva el desempeño de los servicios proporcionados por Bestel
- Procurar que los servicios le sean proporcionados con la calidad prevista.

Operbes S.A. de C.V. tomó en consideración que de conformidad con lo establecido en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el Instituto aplicará penas convencionales por el atraso en el cumplimiento de las fechas pactadas de entrega o de la prestación del servicio, las que no excederán del monto de la garantía de cumplimiento del contrato, y serán determinadas en función de los bienes o servicios no entregados o prestados oportunamente.

### 10.1. Penas Convencionales consideradas por Operbes S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que se aplicarán penas convencionales por incumplimiento en el plazo de prestación de los servicios por parte de Operbes S.A. de C.V. del 0.2% por cada día natural de atraso en el inicio de la prestación del servicio, respecto del valor máximo total del contrato.

### 10.2. Servicios de Habilitación, Operación y Transición

Operbes S.A. de C.V. tomó en consideración como alcance de la presente propuesta las siguientes entregas:

**Partida 1.**

| DESCRIPCIÓN DEL NIVEL DE SERVICIO | FECHA DE ENTREGA | PENA CONVENCIONAL MENSUAL | FÓRMULA DE CÁLCULO |
|---|---|---|---|
| Plan de trabajo detallado de los servicios del proyecto | 15 días naturales posteriores a la emisión del fallo | 1% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Documento Compromiso de suscripción de OLAs | 15 días naturales posteriores a la emisión del fallo | 1% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Matriz de Escalación | 15 días naturales posteriores a la emisión del fallo | 1% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y | 15 días naturales posteriores a la emisión del fallo | 1% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| | | | |
|---|---|---|---|
| capacidades para soportar la prestación de los servicios | | | |

### 10.3. Servicios de Seguridad – Continuidad Operativa

Operbes S.A. de C.V. tomó en consideración como alcance de la presente propuesta las siguientes entregas:

**Partida 1**

| DESCRIPCIÓN DEL NIVEL DE SERVICIO | FECHA DE ENTREGA | PENA CONVENCIONAL MENSUAL | FÓRMULA DE CÁLCULO |
|---|---|---|---|
| Documento con el diseño de alto nivel de las soluciones de seguridad a implementar en los centros de datos o donde lo indique el Instituto | 5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Documento con el diseño de bajo nivel de las soluciones de seguridad a implementar en los centros de datos o donde lo indique el Instituto | 10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Memorias técnicas iniciales de las soluciones de seguridad implementadas | 10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Memorias técnicas actualizadas de los servicios de seguridad | 20 días hábiles previo al término del contrato para aquellos | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio |



ANEXOS
DIVISIÓN DE CONTRATOS

| | | | |
|---|---|---|---|
| | servicios que se encuentren habilitados | | relacionado con el incumplimiento |

### 10.4. Servicios de Seguridad – Verificación/Calidad

## Partida 1

Operbes S.A. de C.V. tomó en consideración como alcance de la presente propuesta las siguientes entregas:

| DESCRIPCIÓN DEL NIVEL DE SERVICIO | FECHA DE ENTREGA | PENA CONVENCIONAL MENSUAL | FÓRMULA DE CÁLCULO |
|---|---|---|---|
| Documento con el diseño de Alto Nivel de los servicios de Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integran activos de infraestructura para su habilitación | 5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto | 10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integran activos de infraestructura para su habilitación | 10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| DESCRIPCIÓN DEL NIVEL DE SERVICIO | FECHA DE ENTREGA | PENA CONVENCIONAL MENSUAL | FORMULA DE CÁLCULO |
|---|---|---|---|
| | | | |
| Memorias Técnicas Actualizadas de las Servicios de Seguridad que requieran integran activos de infraestructura para su habilitación | 20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| <u>Procedimientos de Operación del servicio</u><br>• Servicios de Borrado Seguro de Información<br>• Servicio de Gestión de Dominios<br>• Servicio de Certificados Digitales SSL<br>• Servicios de Ciberinteligencia<br>• Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos móviles<br>• Servicios de Antivirus<br>• Servicios de Prevención de Perdida de Información | 10 días hábiles posteriores a la integración de las mesas de trabajo | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Metodología de implementación de los servicios.<br>• Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)<br>• Servicios de Gestión del Cambio en | 10 días hábiles posteriores a la integración de las mesas de trabajo | 2% por cada día hábil de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| DESCRIPCIÓN DEL NIVEL DE SERVICIO | FECHA DE ENTREGA | PENA CONVENCIONAL MENSUAL | FÓRMULA DE CÁLCULO |
|---|---|---|---|
| Seguridad de la Información | | | |

### 10.5. Servicios del Centro de Operaciones de Seguridad (SOC)

### Partida 1

Operbes S.A. de C.V. tomó en consideración como alcance de la presente propuesta las siguientes entregas:

| DESCRIPCIÓN DEL NIVEL DE SERVICIO | FECHA DE ENTREGA | PENA CONVENCIONAL MENSUAL | FÓRMULA DE CÁLCULO |
|---|---|---|---|
| Procesos de operación implementados:<br>• Requerimientos<br>• Cambios<br>• Configuraciones<br>• Incidentes<br>• Problemas<br>• Monitoreo | 15 días naturales posteriores a la emisión del fallo | 2% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Matriz de Escalación Técnica y Organizacional | 15 días naturales posteriores a la emisión del fallo | 2% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Procedimiento de operación de la Mesa de Servicios:<br>• Requerimientos<br>• Cambios<br>• Configuraciones<br>• Incidentes<br>• Problemas<br>• Monitoreo | 15 días naturales posteriores a la emisión del fallo | 2% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Expedientes Curriculares del personal del SOC | 15 días naturales posterior a la emisión del fallo | 2% por cada día natural de atraso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

### 10.6. Deducciones

Operbes S.A. de C.V. tomó en consideración que durante la vigencia del contrato, al presentarte una falla, incidente, atención de requerimientos, ventana de mantenimiento, entre otras, cuya causa raíz haya sido derivada por un tercero, la deductiva correspondiente al servicio asociado no será aplicada Operbes S.A. de C.V. , siempre y cuando demuestre con evidencias fehacientes que el servicio correspondiente se presentó bajo las especificaciones del anexo técnico, términos y condiciones y los apéndices A y B.

Con base en lo anterior, y cuando las fallas, incidentes, atención de requerimientos, ventanas de mantenimiento, entre otras, sean atribuibles a la entrega de los servicios de seguridad por parte Operbes S.A. de C.V. , se aplicarán deductivas conforme lo siguiente rubros:

**10.7. Disponibilidad**

## Partida 1

Operbes S.A. de C.V. tomó en consideración que la disponibilidad se define como la medida del porcentaje de tiempo, en que el sistema que brinda el servicio de seguridad de SASI 2022-2024, (o un componente del sistema) realiza la función que le es propia. Es decir; disponibilidad es la proporción de tiempo en que el sistema cumple con la función para la cual está dispuesto, en relación con el tiempo en que debería haber estado disponible.

Las mediciones de disponibilidad deberán ser realizadas por Operbes S.A. de C.V. para SASI 2022-2024, usando su correspondiente herramienta de monitoreo del servicio y herramienta de gestión de incidentes, con el afán de obtener mediciones precisas con respecto a los tiempos operacionales y los no operacionales y sus atribuibles.
Operbes S.A. de C.V. tomó en consideración que se realizarán mediciones de disponibilidad desde el inicio del período operacional de los servicios de infraestructura SASI 2022-2024, para todos los módulos o posiciones de servicio contratados.

Operbes S.A. de C.V. como proveedor de SASI 2022-2024, compromete la disponibilidad en base a los siguientes factores:

Incluye todos los componentes WAN, LAN, dispositivos de seguridad, y demás dispositivos que soportan al servicio de seguridad, así como su equivalente de configuración lógica.

Operbes S.A. de C.V. tomó en consideración que la disponibilidad solo será medida sobre los equipos de seguridad solicitados en el anexo técnico de las bases de la licitación.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 504 de la empresa Scitum, S.A. de C.V.

El origen de medición será por una correlación de los poleos y/o muestras recolectadas cada 5 minutos por el sistema de monitoreo y los períodos de indisponibilidad extraídos de los incidentes abiertos en el sistema de administrador de incidencias del proveedor de SASI 2022-2024, restándosele aquellos períodos de indisponibilidad cuya responsabilidad no sea atribuible a Operbes S.A. de C.V. como proveedor de SASI 2022- 2024. La forma de medición propuesta en específico se describe de la siguiente manera.

- Calculada en base a 30 días por mes
- Calculada a partir del inicio de la falla
- Se considera indisponible cuando el protocolo de la interfaz se encuentra caído (Down) o por caída de tráfico imputable a infraestructura del proveedor.
- Solo es calculada en base a fallas imputables al Proveedor de SASI 2022-2024.

<u>Disponibilidad por sitio y por posición de servicio</u>

Las caídas originadas por falla de energía responsabilidad del Instituto no serán tomadas en cuenta para la disponibilidad.

$$\text{Disponibilidad\_del\_Servicio} = \left[\frac{\text{Tiempo\_Total} - (\text{Tiempo\_Indisponible} - \text{Tiempo\_Instituto})}{\text{Tiempo\_Total}}\right] X100$$

Dónde:
Tiempo Total: Tiempo total de disponibilidad para el mes de medición.
Tiempo Indisponible: Tiempo indisponible según plataforma de monitoreo.
Tiempo Instituto: Tiempos atribuibles al Instituto extraídos del sistema de administración de incidentes.

**Objetivos por métrica:**

| Disponibilidad Servicio | % Disponibilidad |
|---|---|
| Servicios de Seguridad – Continuidad Operativa | 99.99% |
| Servicios de Seguridad – Verificación y Calidad | 99.97% |
| Servicios del Centro de Operaciones de Seguridad (SOC) | 99.99% |

Operbes S.A. de C.V. tomó en consideración que Dentro de los servicios solicitados en la sección de "Continuidad Operativa" se encuentran servicios solicitados en standalone, se tendrá que considerar 2 equipos en HA para poder cumplir con la disponibilidad de 99.99% y en caso de no considerarse más que 1 equipo, no aplicará ese nivel de servicio.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, preguntas 505 y 506 de la empresa Scitum, S.A. de C.V.

**Deductiva por incumplimiento**

Operbes S.A. de C.V. tomó en consideración que podrán ser aplicadas las siguientes deductivas:

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FORMULA DE CÁLCULO |
|---|---|---|---|---|
| Cuando no se cumplan con los objetivos de servicio, para los diferentes niveles de disponibilidad, conforme al esquema de medición propuesto | % Disponibilidad conforme la tabla de objetivos | Minuto | 0.5% por cada minuto de indisponibilidad | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

**10.8. Tiempo propuesto para detección y solución de fallas propuestos.**

## Partida 1

Operbes S.A. de C.V. tomó en consideración que la métrica de tiempo de solución a fallas es independiente de la métrica de disponibilidad, dado que se refiere al tiempo en el cual será devuelta a la normalidad (restitución de la operación estable) uno o varios servicios al presentarse una falla. Las mediciones de Tiempo de Solución de Fallas deberán ser realizadas por Operbes S.A. de C.V. como proveedor de SASI 2022-2024, usando su correspondiente herramienta de gestión y monitoreo del servicio. Operbes S.A. de C.V. realizará esta medición en un periodo mensual considerando el promedio del tiempo de solución para cada tipo de severidad. La metodología que se realice, las herramientas y los responsables sobre las mediciones, quedarán definidos en las mesas de trabajo.

El Tiempo de Solución a Fallas se divide en tres casos, en función de la severidad, causa e impacto de los mismos:

**Severidad Critica**: Representa un incidente de alto impacto dado el riesgo que representa. Este tipo de incidente puede, potencialmente, ocasionar afectación y daño en activos y servicios del cliente. Eventos de afectación total al servicio, pérdida total del sistema de comunicaciones y/o seguridad, degradación de los recursos del Instituto o bien mediante el descubrimiento de vulnerabilidad en la infraestructura protegida. La alarma relativa en el sistema de gestión se mantiene por más de 10 minutos.

**Severidad Alta**: Representa un incidente serio en el que hay una degradación más no una afectación de negocio a los servicios e infraestructura que es protegida mediante los dispositivos de alta disponibilidad o de seguridad. El incidente se manifiesta mediante el bloqueo o bajo desempeño al acceder a ciertos servicios de red que requieren el uso de los dispositivos de comunicaciones y/o seguridad, así como la pérdida parcial de alguna funcionalidad en el equipo de comunicaciones y/o seguridad. Eventos de afectación que ocasionan degradación en el servicio sin llegar a ocasionar caída del mismo.

**Severidad Media**: Representa un incidente menor que no trae consecuencias de impacto de negocio a los servicios e infraestructura protegida por los dispositivos de seguridad. El incidente se da mediante fallas en visualización de bitácoras o problemas para comunicación de servicios internos del Instituto y hacia un grupo reducido de usuarios. Eventos de afectación al servicio por períodos de tiempo menores a 10 minutos ocasionando intermitencia en la disponibilidad del servicio.

**Severidad Baja**: Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad. Estos casos de severidad serán atendidos por ingenieros de Operbes S.A. de C.V. en sitio con la colaboración del fabricante vía un centro de asistencia técnica personalizada. El tiempo de resolución de este tipo de falla será definido por el Instituto Operbes S.A. de C.V. como proveedor de SASI 2022-2024, al momento de presentar el caso.

Operbes S.A. de C.V. tomó en consideración que la severidad de un incidente es determinada por la convocante. Conforme la operación y criticidad de un servicio, se define la severidad, así como su nivel de escalación, con base en lo siguiente:

| SEVERIDAD | AFECTACIÓN | TIEMPO MÁXIMO DE REGISTRO | TIEMPO MÁXIMO DE SOLUCIÓN |
|---|---|---|---|
| **Critica** | Representa una falla de alto impacto que impide la operación total de un servicio, mismo que soporta una función de negocio del Instituto a nivel nacional. | 10 minutos posteriores a la detección de la falla | 2 horas posteriores al registro y notificación de la falla |
| **Alta** | Representa una falla en la que hay una degradación que impide la operación de un servicio, mismo que soporta una función de negocio del Instituto pero que no tiene un impacto a nivel nacional. | 20 minutos posterior a la detección de la falla | 4 horas posterior al registro y notificación de la falla |
| **Media** | Representa una falla menor que impide la operación de un servicio, mismo que afecta a un grupo de usuarios reducido del Instituto. | 120 minutos posterior a la detección de la falla | 48 horas posterior al registro y notificación de la falla |
| **Baja** | Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad, tienen un bajo impacto en la operación del negocio y su atención y/o solución puede ser calendarizada. | 5 días hábiles posterior a la detección de la falla | Se define entre el Instituto y el Proveedor de SASI 2022-2024 conforme las mesas de trabajo que se establezcan para este propósito. |

**Deductivas por incumplimiento**

Operbes S.A. de C.V. tomó en consideración que podrán ser aplicadas las siguientes deductivas:

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Tiempo máximo de registro y notificación | 10 minutos posteriores al registro y | Minuto | 0.2% por cada minuto de atraso en el | Valor unitario de la facturación mensual del servicio |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| conforme al nivel de severidad critica | notificación de la falla | | registro y notificación | relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad critica | 2 horas posteriores al registro y notificación de la falla | Hora | 0.5% por cada hora o fracción de atraso en la solución de la falla | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de severidad alta | 20 minutos posteriores al registro y notificación de la falla | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad alta | 4 horas posteriores a la registro y notificación de la falla | Hora | 0.5% por cada hora o fracción de atraso en la solución de la falla | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de severidad media | 120 minutos posteriores al registro y notificación de la falla | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad media | 48 horas posteriores al registro y notificación de la falla | Hora | 0.5% por cada hora o fracción de atraso en la solución de la falla | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel | 5 días hábiles posteriores al registro y notificación de la falla | Día | 0.2% por cada día hábil de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCION DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FORMULA DE CALCULO |
|---|---|---|---|---|
| de severidad baja | | | | |
| Tiempo máximo de solución conforme al nivel de severidad baja | Se define entre el Instituto y el Proveedor de SASI 2022-2024 conforme las mesas de trabajo que se establezcan para este propósito. | Día | 0.5% por cada día de atraso en la solución de la falla conforme la fecha establecida en las mesas de trabajo | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

**10.9. Tiempo propuesto para detección y mitigación de incidentes**

**Partida 1**

Operbes S.A. de C.V. tomó en consideración que una actividad sospechosa son acciones que pudieran estar encaminadas a comprometer la seguridad de la red y de los activos de información, es la etapa previa a la materialización de un incidente de seguridad. Un incidente de seguridad es el registro de una violación a las políticas de seguridad informática o al uso aceptable de políticas o de prácticas de seguridad estandarizado; es la evidencia inequívoca de que la confidencialidad, integridad y disponibilidad de la información ha sido vulnerada.

Las métricas de tiempo para la actividad sospechosa se refieren al tiempo de notificación y envió de dictamen que Operbes S.A. de C.V. en caso de ser el proveedor SASI 2022-2024 realizará ante el Instituto al momento de detectar una actividad sospechosa. Ante una actividad sospechosa, Operbes S.A. de C.V. en caso de ser el proveedor del SASI 2022-2024 registrará y notificará al personal del Instituto en máximo 30 minutos. Posterior a su detección y registro, se emitirá un dictamen de actividad sospechosa con recomendaciones para erradicarla, este dictamen será enviado al personal del Instituto en máximo 90 minutos.

Las métricas para el tiempo de registro y notificación se refieren al tiempo en que Operbes S.A. de C.V. en caso de ser el proveedor SASI 2022-2024 avisa al Instituto cuando ha confirmado un incidente de seguridad, ésta métrica se realizará en los tiempos definidos según la prioridad a partir de que se apertura algún registro relacionado con un incidente de seguridad. La métrica de tiempo de contención se refiere a que, tras la detección del incidente, Operbes S.A. de C.V. en caso de ser el Proveedor de SASI 2022-2024 detendrá y aislará el mismo según los tiempos definidos para cada prioridad.

Las mediciones serán realizadas por Operbes S.A. de C.V. en caso de ser el proveedor de SASI 2022-2024, usando su correspondiente herramienta de gestión y monitoreo del servicio. Operbes S.A. de C.V. realizará esta medición en un periodo mensual según el nivel de servicio para cada tipo de métrica y/o prioridad.

**Objetivos de la métrica**

Operbes S.A. de C.V. tomó en consideración los siguientes tipos de métricas:

| SEVERIDAD | AFECTACIÓN | TIEMPO MAXIMO DE REGISTRO | TIEMPO MAXIMO DE SOLUCION |
|---|---|---|---|
| **Critica** | Representa un incidente de alto impacto que impide la operación total de un servicio, mismo que soporta una función de negocio del Instituto a nivel nacional. | 10 minutos posteriores a la detección del incidente | 60 minutos posteriores al registro y notificación del incidente |
| **Alta** | Representa un incidente en el que hay una degradación que impide la operación de un servicio, mismo que soporta una función de negocio del Instituto pero que no tiene un impacto a nivel nacional. | 20 minutos posterior a la detección del incidente | 240 minutos posteriores al registro y notificación del incidente |
| **Media** | Representa un incidente menor que impide la operación de un servicio, mismo que afecta a un grupo de usuarios reducido del Instituto. | 30 minutos posterior a la detección del incidente | 60 minutos posteriores al registro y notificación del incidente |
| **Baja** | Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad, tienen un bajo impacto en la operación del negocio y su atención y/o | 60 minutos posterior a la detección del incidente | 2,880 minutos posteriores al registro y notificación del incidente |

| SEVERIDAD | AFECTACIÓN | TIEMPO MÁXIMO DE REGISTRO | TIEMPO MÁXIMO DE SOLUCIÓN |
|---|---|---|---|
| | solución puede ser calendarizada. | | |

**Deductiva por incumplimiento**

Operbes S.A. de C.V. tomó en consideración las siguientes deductivas por incumplimiento :

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Registro y notificación de Actividad Sospechosa | 30 minutos posteriores a la detección actividad sospechosa | Minuto | 0.5% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Envío de Dictamen de Actividad Sospechosa | 90 minutos posteriores al registro y notificación de actividad sospechosa | Minuto | 1% por cada minuto de atraso en la elaboración del dictamen | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Tiempo máximo de registro y notificación conforme al nivel de severidad critica | 10 minutos posteriores al registro y notificación del incidente | Minuto | 0.5% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad critica | 60 minutos posteriores al registro y notificación del incidente | Minuto | 1% por cada minuto de atraso en la solución del incidente | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y | 20 minutos posteriores al | Minuto | 0.5% por cada minuto de | Valor unitario de la facturación |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| notificación conforme al nivel de severidad alta | registro y notificación del incidente | | atraso en el registro y notificación | mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad alta | 240 minutos posteriores al registro y notificación del incidente | Minuto | 1% por cada minuto de atraso en la solución del incidente | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de severidad media | 30 minutos posteriores al registro y notificación del incidente | Minuto | 0.5% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad media | 1,440 minutos posteriores al registro y notificación del incidente | Minuto | 1% por cada minuto de atraso en la solución del incidente | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de severidad baja | 60 minutos posteriores al registro y notificación del incidente | Minuto | 0.5% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de severidad baja | 2,880 minutos posteriores al registro y notificación del incidente | Minuto | 1% por cada minuto de atraso en la solución del incidente | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

**10.10. Solicitudes de requerimientos y cambios**

**Partida 1**

Es el tiempo que tarda Operbes S.A. de C.V. en caso de ser el Proveedor de SASI 2022-2024, en realizar una alta, cambio o baja sobre la infraestructura del servicio en seguridad, basada en el menú de configuraciones comunes preestablecidas durante las mesas de trabajo correspondientes. Estas

configuraciones serán acorde a las necesidades de conectividad y flujos de información de las aplicaciones del Instituto, entendiendo que la complicación para su atención es menor dado que se tiene la experiencia y el conocimiento de las mismas configuraciones de los módulos de los servicios de seguridad en operación.

**Objetivos de la métrica:**

| PRIORIDAD | DESCRIPCIÓN | TIEMPO MÁXIMO DE REGISTRO | TIEMPO MÁXIMO DE EJECUCIÓN |
|---|---|---|---|
| **Alta** | Requerimiento generado por parte del Instituto a fin de atender a necesidades de operación emergentes. | 10 minutos posteriores a la solicitud formal por parte del Instituto | 60 minutos posteriores al registro realizado por el Instituto |
| **Media** | Requerimiento generado por parte del Instituto a fin de atender a necesidades de operación comunes. | 30 minutos posteriores a la solicitud formal por parte del Instituto | 480 minutos posteriores al registro realizado por el Instituto |
| **Baja** | Requerimiento generado por parte del Instituto a fin de atender a necesidades de operación programadas. | 60 minutos posteriores a la solicitud formal por parte del Instituto | 1,440 minutos posteriores al registro realizado por el Instituto |

**Cambios**

| PRIORIDAD | DESCRIPCIÓN | TIEMPO MÁXIMO DE REGISTRO | TIEMPO MÁXIMO DE EJECUCIÓN |
|---|---|---|---|
| **Emergente** | Cambios requeridos como resultado de una pérdida repentina del servicio, falla en un activo de infraestructura o a petición del Instituto. | 1 hora posteriores a la solicitud formal por parte del Instituto | Conforme al plan de trabajo definido entre el Instituto y el Proveedor |
| **Normal** | Cambios solicitados para mejorar o restaurar un servicio o ampliar un activo de | 1 hora posteriores a la solicitud formal por | Conforme al plan de trabajo definido entre el Instituto y el Proveedor |

| PRIORIDAD | DESCRIPCIÓN | TIEMPO MÁXIMO DE REGISTRO | TIEMPO MÁXIMO DE EJECUCIÓN |
|---|---|---|---|
| | infraestructura, que no están considerados en el catálogo de cambios estándar, mismos que deben ser analizados y aprobados por el Instituto. | parte del Instituto | |
| **Estándar** | Cambios en los servicios y/o activos de infraestructura que se realiza en línea y sigue una trayectoria establecida, mismos que representan una solución aceptada a un requerimiento o conjunto de requerimientos específicos. | 1 hora posteriores a la solicitud formal por parte del Instituto | 24 horas posterior al registro realizado por el Instituto |

Cualquier cambio ejecutado por Operbes S.A. de C.V. , mismo que no se encuentre autorizado por el Instituto, derive o no en alguna falla de los servicios de seguridad, será catalogado como un incidente de seguridad, mismo que será clasificado con base en las afectaciones o riesgos que pudieron generar.

**Deductiva por incumplimiento:**

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Tiempo máximo de registro y notificación conforme al nivel de prioridad Alta | 10 minutos posteriores al registro y notificación del requerimiento | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de ejecución conforme al nivel de prioridad Alta | 60 minutos posteriores al registro y notificación del requerimiento | Minuto | 0.5% por cada minuto de atraso en la ejecución del requerimiento | Valor unitario de la facturación mensual del servicio relacionado con |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FORMULA DE CALCULO |
|---|---|---|---|---|
| | | | | el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de prioridad Media | 30 minutos posteriores al registro y notificación del requerimiento | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de prioridad Media | 8 horas posteriores al registro y notificación del requerimiento | Hora | 0.5% por cada hora o fracción de atraso en la ejecución del requerimiento | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de prioridad Baja | 60 minutos posteriores al registro y notificación del requerimiento | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de prioridad Baja | 24 horas posteriores al registro y notificación del requerimiento | Hora | 0.5% por cada hora o fracción de atraso en la ejecución del requerimiento | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

**Cambios**

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FORMULA DE CÁLCULO |
|---|---|---|---|---|
| Tiempo máximo de registro y notificación conforme al nivel | 60 minutos posteriores al registro y | Minuto | 0.2% por cada minuto de atraso en el | Valor unitario de la facturación mensual del servicio |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| de prioridad Emergente | notificación del cambio | | registro y notificación | relacionado con el incumplimiento |
| Tiempo máximo de ejecución conforme al nivel de prioridad Emergente | Conforme al plan de trabajo definido entre el Instituto y el Proveedor | Hora | 1% por cada hora o fracción de atraso en la ejecución del cambio | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de prioridad Normal | 60 minutos posteriores al registro y notificación del cambio | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de prioridad Normal | Conforme al plan de trabajo definido entre el Instituto y el Proveedor | Hora | 1% por cada hora o fracción de atraso en la ejecución del cambio | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de registro y notificación conforme al nivel de prioridad Estándar | 60 minutos posteriores al registro y notificación del cambio | Minuto | 0.2% por cada minuto de atraso en el registro y notificación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tiempo máximo de solución conforme al nivel de prioridad Estándar | 24 horas posteriores al registro y notificación del cambio | Hora | 1% por cada hora o fracción de atraso en la ejecución del cambio | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

**10.11. Servicios de Seguridad – Continuidad Operativa**

**Partida 1**

Operbes S.A. de C.V. tomó en consideración la siguiente tabla:

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Reportes Técnicos de los activos de infraestructura que contemplen:<br>• Disponibilidad<br>• Controles de Cambios<br>• Requerimientos<br>• Incidentes/Fallas<br>• Actividad Sospechosa<br>• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

**10.12. Servicios de Seguridad – Verificación/Calidad**

**Partida 1**

Operbes S.A. de C.V. tomó en consideración la siguiente tabla:

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Reportes Técnicos de los activos de infraestructura que contemplen:<br>• Disponibilidad<br>• Controles de Cambios<br>• Requerimientos<br>• Incidentes/Falla | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| • Actividad Sospechosa<br>• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) | | | | |
| Servicios de Borrado Seguro de Información: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado. | 5 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Servicio de Gestión de Dominios: | 5 días hábiles posteriores a la solicitud | Día | 1% por cada día hábil de atraso en la entrega de los | Valor unitario de la facturación |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FORMULA DE CÁLCULO |
|---|---|---|---|---|
| Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos. | generada por parte del Instituto | | reportes técnicos/ejecutivos | mensual del servicio relacionado con el incumplimiento |
| Servicio de Certificados Digitales SSL: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los certificados que se hayan renovado o adquiridos (incluyendo archivo electrónico compreso con la llave publica relacionado con los requerimientos) | 1 día hábil posterior a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Servicios de Ciberinteligencia: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de amenazas y ataques potenciales a los que se encuentra expuesto el Instituto que incluya: Situación | 1 día hábil posterior a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| general del evento, hallazgos detectados, mecanismos de inteligencia accionable, táctica u operativa recomendados para prevención y/o contención | | | | |
| Servicios de Sistema de Gestión de Seguridad de la Información: Plan de Trabajo de implementación y operación de los servicios conforme al alcance definido en las mesas de trabajo | 10 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del plan de trabajo | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Servicios de Sistema de Gestión de Seguridad de la Información: Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora del Sistemas De Gestión de Seguridad de la Información (SGSI) | Conforme a la fecha estipulada en el plan de trabajo acordado entre el Instituto y el Proveedor | Día | 1% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, por evento | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Servicios de Gestión del | 10 días hábiles | Día | 1% por cada día hábil de atraso en | Valor unitario de la |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Cambio en Seguridad de la Información: Plan de Trabajo de implementación y operación de los servicios conforme al alcance definido en las mesas de trabajo | posteriores a la solicitud generada por parte del Instituto | | la entrega del plan de trabajo | facturación mensual del servicio relacionado con el incumplimiento |
| Servicios de Gestión del Cambio en Seguridad de la Información: Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora de la Gestión del Cambio en Seguridad de la Información | Conforme a la fecha estipulada en el plan de trabajo acordado entre el Instituto y el Proveedor | Día | 1% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, por evento | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

**10.13. Servicios del Centro de Operaciones de Seguridad (SOC)**

Operbes S.A. de C.V. tomó en consideración la siguiente tabla:

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| Reporte Técnico de los requerimientos generados a | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los | Valor unitario de la facturación mensual del servicio |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FORMULA DE CÁLCULO |
|---|---|---|---|---|
| través de la Mesa de Servicios para los servicios de seguridad implementados | | | reportes técnicos | relacionado con el incumplimiento |
| Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las definiciones | 5 días hábiles posteriores al cumplimiento del mes vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes de estadísticas | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| realizadas en las mesas de trabajo | | | | |
| Reporte de las evaluaciones operativas a los servicios de seguridad implementados | 5 días hábiles posteriores al cumplimiento de cada trimestre vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes de estadísticas | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte que integre el calendario de actualizaciones de versionamiento en software de cada servicio implementados | 5 días hábiles posteriores al cumplimiento de cada trimestre vencido | Día | 1% por cada día hábil de atraso en la entrega de los reportes de estadísticas | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Creación de cuentas de acceso en las consolas de administración de los servicios de seguridad | 5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto | Día | 1% por cada día hábil de atraso en la entrega de las cuentas de acceso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad | 5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto | Día | 1% por cada día hábil de atraso en la entrega de las cuentas de acceso | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FORMULA DE CÁLCULO |
|---|---|---|---|---|
| Actualización de la matriz de escalación | 5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad | Día | 1% por cada día hábil de atraso en la entrega de la matriz de escalación | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad | 5 días hábiles posteriores a la ejecución de la ventana mantenimiento | Día | 1% por cada día hábil de atraso en la entrega de los reportes técnicos | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad | 5 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del reporte | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte Técnico de las configuraciones de las soluciones de seguridad | 5 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del reporte técnico | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte Técnico de los incidentes presentados en las soluciones de seguridad | 5 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del reporte técnico | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Reporte Técnico de los requerimientos | 5 días hábiles posteriores a la solicitud | Día | 1% por cada día hábil de atraso en la | Valor unitario de la facturación mensual del |



ANEXOS
DIVISIÓN DE CONTRATOS

| CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO) | NIVEL DE SERVICIO | UNIDAD DE MEDIDA | DEDUCTIVA | FÓRMULA DE CÁLCULO |
|---|---|---|---|---|
| registrados en la mesa de servicios | generada por parte del Instituto | | entrega del reporte técnico | servicio relacionado con el incumplimiento |
| Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y su diagrama de interrelación conforme fueron registrados en la CMDB | 5 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del reporte técnico | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Diagramas de Arquitectura de las soluciones de seguridad | 2 días hábiles posteriores a la solicitud generada por parte del Instituto | Día | 1% por cada día hábil de atraso en la entrega del reporte técnico | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |
| Tablero de Estadísticas de Servicios de Seguridad (Portal Único) | 10 días hábiles posteriores al término de la habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo | Día | 1% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, por evento | Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento |

Operbes S.A. de C.V. tomó en consideración que cualquier cambio ejecutado por el SOC, mismo que no se encuentre autorizado por el Instituto, derive o no en alguna falla de los servicios de seguridad, será catalogado como un incidente de seguridad, mismo que será clasificado con base en las afectaciones o riesgos que pudieron generar.

## 11. Condiciones de Pago

Operbes S.A. de C.V. tomó en consideración que cómo se establece en el presente documento, el administrador de contrato será el servidor público responsable de supervisar que se cumplan en tiempo y forma los compromisos contenidos en el contrato que para tal efecto se celebre.

Operbes S.A. de C.V. tomó en consideración los pagos se realizarán previa validación y aceptación de los servicios por parte del Administrador del Contrato, es decir, el Titular de la División de Seguridad Informática Física, que reciba cada uno de los servicios y que será responsable de realizar los trámites de pago en estricto apego al procedimiento administrativo vigente en el instituto.

Operbes S.A. de C.V. tomó en consideración que para proceder a la liberación de pago, el Titular de la División de Seguridad Informática Física o el Servidor Público que para tal efecto haya designado el Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información, será responsable de la supervisión y administración de todas las obligaciones a cargo del proveedor.

Así como de la ejecución, validación, técnica y administrativamente de todos y cada uno de los documentos que acreditan que los servicios proporcionados por Operbes S.A. de C.V. se cumplieron en tiempo, forma y cantidad con las características, especificaciones y condiciones contractualmente pactadas para el proyecto, procederá de conformidad con lo establecido en el artículo 51 de la LAASSP, la forma de pago a Operbes S.A. de C.V. será la estipulada en los contratos y quedará sujeta a las condiciones que establezcan las mismas; sin embargo, no podrá exceder de veinte días naturales contados a partir de la entrega de la factura respectiva, previa entrega de certificado de licencia o de la prestación de los servicios en los términos del contrato.

Operbes S.A. de C.V. entregará en la División de Trámite de Erogaciones, situada en la calle de Gobernador Tiburcio Montiel No. 15, PB, Col. San Miguel Chapultepec, Código Postal 11850, Delegación Miguel Hidalgo, México, D.F., en días y horas hábiles, los siguientes documentos:

- Original y copia de la factura que expida Bestel, a nombre del Instituto Mexicano del Seguro Social, con dirección en Av. Paseo de la Reforma N° 476, Col. Juárez, Delegación Cuauhtémoc, C.P. 06600, México, D.F., y R.F.C. IMS-421231-I45; que reúna los requisitos fiscales, en la que se indiquen los servicios proporcionados y el número de contrato que ampara dichos servicios,
- Original y Copia de la documentación que avale la entrega de los servicios a satisfacción del instituto (Acta Entrega-Recepción de los Servicios).
- Carta firmada por el representante legal, en la cual haga del conocimiento del instituto la cuenta bancaria a la que se efectuará la transferencia electrónica bancaria correspondiente.
- Nota de crédito (en caso de que aplique) a favor del Instituto Mexicano del Seguro Social por el importe de la sanción en caso de entrega extemporánea de los servicios contratados.
- Presentará Orden de Ingreso (Nota de Crédito) (en caso de que aplique para Soporte Técnico dentro de los primeros 10 días hábiles después de la fecha del Acta Entrega-Recepción de los Servicios del trimestre firmada, a favor del Instituto Mexicano del Seguro Social por el importe de la sanción en caso de entrega extemporánea de los servicios contratados, en caso de no entregar la Orden de ingreso (Nota de Crédito) correspondiente al plazo citado en este punto, se aplicara la ejecución de garantía.

En caso de que Operbes S.A. de C.V. presente sus facturas con errores o deficiencias, estos se le harán saber por parte del instituto dentro del término estipulado para ello, y el plazo de pago se ajustará,

presentará nuevamente toda la documentación mencionada anteriormente (en original y/o copia, según corresponda).

El Pago se realizará en pesos mexicanos, en pagos progresivos a mes vencido conforme a las entregas programadas.

## 12. Entregables

Operbes S.A. de C.V. entregará al Titular de la División de Seguridad Informática Física dependiente de la Coordinación de Telecomunicaciones y Seguridad de la Información los siguientes:

### 12.1. Entregables Generales

**Partida 1**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Habilitación, Operación y Transición | Plan de Trabajo Detallado de los servicios del proyecto | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Documento Compromiso de suscripción del acuerdo de niveles operacional (*Operational Level Agreement,* OLA) | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Matriz de Escalación | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Escrito por parte de Operbes S.A. de C.V. , firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| Servicios de Seguridad – Continuidad Operativa | Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto | Única Vez | 5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Documento con el diseño de Bajo Nivel | Única Vez | 10 días hábiles posteriores a la |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto | | integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas | Única Vez | 10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo |
| | Memorias Técnicas Actualizadas de las Servicios de Seguridad | Única Vez | 20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados |
| Servicios de Seguridad – Verificación/Calidad | Documento con el diseño de Alto Nivel de los servicios de Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integran activos de infraestructura para su habilitación | Única Vez | 5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar |
| | Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integran activos de | Única Vez | 10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | infraestructura para su habilitación | | donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo |
| | Memorias Técnicas Actualizadas de las Servicios de Seguridad, que requieran integran activos de infraestructura para su habilitación | Única Vez | 20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados |
| Servicios de Borrado Seguro de Información | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicio de Gestión de Dominios | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicio de Certificados Digitales SSL | Procedimientos de Operación del servicio | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Sistema de Gestión de Seguridad de la Información (SGSI) | Metodología para la continuidad de los servicios | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios de Gestión del Cambio en Seguridad de la Información | Metodología para la implementación de los servicios | Única Vez | 10 días hábiles posteriores a la integración de las mesas de trabajo |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Procesos de operación implementados:<br>• Requerimientos<br>• Cambios<br>• Configuraciones<br>• Incidentes<br>• Problemas<br>• Monitoreo | Única Vez | 15 días naturales posteriores a la emisión del fallo |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | Matriz de Escalación Técnica y Organizacional | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Procedimiento de operación de la Mesa de Servicios:<br>• Requerimientos<br>• Cambios<br>• Configuraciones<br>• Incidentes<br>• Problemas<br>• Monitoreo | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| | Expedientes Curriculares del personal del SOC | Única Vez | 15 días naturales posteriores a la emisión del fallo |
| Tablero de Estadísticas de Servicios de Seguridad (Portal Único) | Creación de cuentas de acceso en portal único de las soluciones de seguridad | Única Vez | 10 días hábiles posteriores al término de la habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo |

### 12.2. Entregables bajo demanda

Bestel, de manera enunciativa más no limitativa, generará entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

**Partida 1**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Borrado Seguro de Información | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado. | | |
| Servicio de Gestión de Dominios | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos. | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicio de Certificados Digitales SSL | Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los certificados que se hayan renovado o adquiridos (incluyendo archivo electrónico compreso con la llave publica relacionado con los requerimientos) | Evento | 1 día hábil posteriores a la solicitud generada por parte del Instituto |
| Servicios de Sistema de Gestión de Seguridad de la Información | Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo | Evento | 10 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicios de Gestión del Cambio en Seguridad de la Información | Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo | Evento | 10 días hábiles posteriores a la solicitud generada por parte del Instituto |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad | Evento | 5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | | | conforme a cada solicitud generada por el Instituto |
| | Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad | Evento | 5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme cada solicitud generada por el Instituto |
| | Actualización de la matriz de escalación | Evento | 5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad y Red |
| | Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad y red | Evento | 5 días hábiles posteriores a la ejecución de la ventana mantenimiento |
| | Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad y red | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Reporte Técnico de las configuraciones de las soluciones de seguridad y red | Evento | 5 días hábiles posterior a la solicitud generada por parte del Instituto |
| | Reporte Técnico de los incidentes presentados en las soluciones de seguridad y red | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Reporte Técnico de los requerimientos registrados en la mesa de servicios | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y red, así como su diagrama de | Evento | 5 días hábiles posteriores a la solicitud generada por parte del Instituto |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | interrelación conforme fueron registrados en la CMDB | | |
| | Diagramas de Arquitectura de las soluciones de seguridad y red | Evento | 2 días hábiles posteriores a la solicitud generada por parte del Instituto |
| | | | |

### 12.3. Entregables Periódicos

Bestel, de manera enunciativa más no limitativa, generará entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

**Partida 1**

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| Servicios de Seguridad – Continuidad Operativa | Reportes Técnicos de los activos de infraestructura que contemplen:<br>• Disponibilidad<br>• Controles de Cambios<br>• Requerimientos<br>• Incidentes/Fallas<br>• Actividad Sospechosa<br>• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| Servicios de Seguridad – Verificación/Calidad | Reportes Técnicos de los activos de infraestructura que contemplen:<br>• Disponibilidad<br>• Controles de Cambios<br>• Requerimientos<br>• Incidentes/Fallas<br>• Actividad Sospechosa<br>• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| Servicios del Centro de Operaciones de Seguridad (SOC) | Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |

| SERVICIO | ENTREGABLE | PERIODICIDAD | ENTREGA |
|---|---|---|---|
| | servicios de seguridad implementados | | |
| | Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo | Mensual | 5 días hábiles posteriores al cumplimiento del mes vencido |
| | Reporte de las evaluaciones operativas a los servicios de seguridad implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |
| | Reporte que integre el calendario de actualizaciones de versionamiento en *software* de cada servicio implementados | Trimestral | 5 días hábiles posteriores al cumplimiento de cada trimestre calendario |

Los entregables requeridos durante la vigencia del contrato, serán entregados en formato electrónico (MS Word, MS Excel, PDF) conforme los periodos estipulados por el Instituto.

De igual manera, Operbes S.A. de C.V. establecerá un repositorio digital, que, de manera alterna, servirá para alojar los entregables antes señalados, mismos que estarán disponibles para su consulta durante la vigencia del contrato, teniendo en cuenta que el Instituto definirá en las mesas de trabajo los permisos de acceso correspondientes para el administrador del contrato, cuerpo de gobierno que se conforme para este propósito u otros funcionaros que sean designados por el primero mencionado.

## 13. Condiciones de aceptación de los servicios

1. Se deberán formalizar los entregables descritos en el numeral anterior a efecto de dar por recibido los servicios requeridos.

2. Todos los documentos serán entregados en papel membretado de la empresa de manera impresa y en electrónico.

3. Se entregará a la División de Seguridad Informática Física perteneciente a la Coordinación de Telecomunicaciones y Seguridad de la Información.

## 14. Lugar y horario para la entrega

- Operbes S.A. de C.V. tomó en consideración que la entrega se realizará en las instalaciones del Instituto ubicadas en la calle de Avenida Paseo de la Reforma 476, Anexo de Telecomunicaciones Planta Alta, Colonia Juárez, Delegación Cuauhtémoc, Ciudad de México, C.P. 06600.
- Operbes S.A. de C.V. tomó en consideración que el horario para la entrega será de las 9:00 horas a las 17:00 horas
- Operbes S.A. de C.V. tomó en consideración que en caso de contingencia podrá solicitarse la entrega de las cartas requeridas en el presente documento en cualquiera de los inmuebles que formen parte de las Oficinas Centrales del instituto, ubicadas en la Colonia Juárez, Delegación Cuauhtémoc, C.P. 06600 en la Ciudad de México.

## 15. Convenio de Confidencialidad y Resguardo de la Información

Operbes S.A. de C.V. suscribirá el Convenio de Confidencialidad y Resguardo de Información Correspondiente con la persona designada como Administradora de Contrato. En complemento, Operbes S.A. de C.V. considerará al menos los siguientes mecanismos de control de acceso a la información del IMSS:

a. Se establecerá controles de acceso y privilegios restringidos al personal de Operbes S.A. de C.V. , a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del IMSS.

b. Operbes S.A. de C.V. implantará y aceptará en todo momento el uso de controles que permitan "Pistas de Auditoria" para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.

c. La seguridad lógica estará protegida mediante el uso de "Firewalls", mecanismos de encriptación y seguridad física entre las redes de Operbes S.A. de C.V. y las del IMSS.

d. Operbes S.A. de C.V. contará con sistemas que contengan una administración estricta de registros y políticas de retención de la información del IMSS.

e. Los empleados de Operbes S.A. de C.V. con acceso a la información sensible del IMSS, firmarán acuerdos de confidencialidad con este.

f. El almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por Operbes S.A. de C.V. en caso de ser el proveedor de los servicios de SASI 2022-2024 observando los requisitos de seguridad y resguardo de la información.

g. El uso de *hardware* que podría ser utilizado para copiar datos y extraer información, como son dispositivos removibles, quemado de CD y dispositivos de memoria "Flash-USB", entre otros, por parte del personal de Operbes S.A. de C.V. serán restringidos y observará las políticas de seguridad del IMSS al respecto.

h. Operbes S.A. de C.V. permitirá el acceso a información relacionada con el servicio prestado al IMSS para la realización de auditorías.

i. Operbes S.A. de C.V. no hará uso indebido de la documentación, información, ni activos de TIC a los que tengan acceso o que se generen con motivo de la prestación del servicio.

**16. Propiedad Intelectual**

Operbes S.A. de C.V. se obliga durante la garantía de las licencias a liberar a el Instituto de toda responsabilidad de carácter civil, mercantil, penal o administrativa que, en su caso, se ocasione con motivo de la infracción de derechos de autor, patentes, marcas u otros derechos de propiedad industrial o intelectual a nivel Nacional o Internacional.

**17. Método de evaluación de propuestas**

Operbes S.A. de C.V. tomó en consideración que se evaluará mediante el procedimiento de puntos y porcentajes, conforme a las características que presenten los proveedores en cuanto a funcionalidades requeridas en el Anexo Técnico, de acuerdo con la ponderación establecida en la matriz de evaluación correspondiente.

**18. Funcionarios públicos de la DIDT participantes en el proceso de contratación**

Operbes S.A. de C.V. tomó en consideración los siguientes funcionarios:

a) C. Florencio Fernando González Velázquez, Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información.
b) C. Abraham Gutiérrez Castillo, Titular de la División de Seguridad Informática Física.
c) C. Cynthia Osmara Verdin Villegas, Jefe Área Nivel Central.

**19. Vigencia del Contrato**

Operbes S.A. de C.V. tomó en consideración que la vigencia del contrato será a partir del día hábil siguiente a la notificación del fallo y hasta el 30 de septiembre de 2024.

**20. Plazo del servicio**

Operbes S.A. de C.V. tomó en consideración que la prestación de los servicios iniciará a partir del día hábil siguiente a la notificación del fallo y hasta el 30 de septiembre de 2024.

Operbes S.A. de C.V. tomó en consideración que los periodos de implementación y transición del servicio serán acordados en una mesa de trabajo entre el Licitante adjudicado y el instituto, privilegiando en todo momento la continuidad operativa de los servicios.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 169 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que durante el período de implementación no aplicaran las deducciones correspondientes.
Operbes S.A. de C.V. tomó en consideración que es importante resaltar, que las mesas de trabajo entre el proveedor adjudicado y el administrador del contrato, con la finalidad de establecer el periodo de transición, así como los temas operativos resultantes de este.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, pregunta 170 de la empresa Axtel, S.A.B. de C.V.

Operbes S.A. de C.V. tomó en consideración que los periodos de la habilitación e implementación del servicio serán mínimo 30 días naturales y máximo 90 días naturales. Operbes S.A. de C.V. tomó en consideración que se reitera para este tema en específico se realizara mesa de trabajo entre el licitante adjudicado y el Instituto , privilegiando en todo momento la continuidad de los servicios.

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 53 de la empresa Axtel, S.A.B. de C.V.

## 21. Administrador del Contrato

Operbes S.A. de C.V. tomó en consideración que conforme a las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto, el Administrador del Contrato, será el responsable de supervisar que se cumplan en tiempo y forma los compromisos contenidos en el contrato que para tal efecto se celebre, por lo que:

a) **Administrador del Contrato y Responsable Técnico**; Titular de la División de Seguridad Informática Física.

b) **Supervisor del Contrato**; Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información.

Operbes S.A. de C.V. tomó en consideración que los servicios a cargo del proveedor estarán bajo la administración y supervisión del responsable designado que para tal efecto.

## 22. Mecanismos de control para la administración del contrato

El Administrador del Contrato en conjunto con Operbes S.A. de C.V. generará el acta de entrega-recepción conforme a lo establecido en el Anexo Técnico de las bases de la licitación.

## 23. Mecanismos requeridos al proveedor para responder por defectos o vicios ocultos de los bienes o de la calidad de los servicios

Operbes S.A. de C.V. tomó en consideración que no aplica

## 24. Otorgamiento de anticipo

Operbes S.A. de C.V. tomó en consideración que no aplica

Operbes S.A. de C.V. tomó en consideración la siguiente tabla que contiene los valores referenciales mínimos y máximos a considerar:

| PARTIDA 1 | | | |
|---|---|---|---|
| No. | Descripción de Servicio | Cantidad Mínima | Cantidad Máxima |
| 1 | Firewall (Tipo 4) | 2 | 4 |
| 2 | Licenciamiento Firewall (Tipo 4) - Implementación | 2 | 4 |
| 3 | Licenciamiento Firewall (Tipo 1) - Renovación | 1 | 1 |
| 4 | Licenciamiento Firewall (Tipo 2) - Renovación | 2 | 2 |
| 5 | Licenciamiento Firewall (Tipo 3) - Renovación | 4 | 4 |
| 6 | Licenciamiento Firewall (Tipo 4) - Renovación | 2 | 2 |
| 7 | IPS (Tipo 3) | 2 | 4 |
| 8 | Licenciamiento IPS (Tipo 3) - Implementación | 2 | 4 |
| 9 | Licenciamiento IPS (Tipo 1) - Renovación | 1 | 1 |
| 10 | Licenciamiento IPS (Tipo 2) - Renovación | 1 | 1 |
| 11 | Licenciamiento IPS (Tipo 3) - Renovación | 2 | 2 |
| 12 | Licenciamiento IPS (Tipo 4) - Renovación | 2 | 2 |
| 13 | Anti-denegación de servicios DDoS (Tipo 2) | 2 | 4 |
| 14 | Licenciamiento Anti-denegación de servicios DDoS (Tipo 2) - Implementación | 2 | 4 |
| 15 | Licenciamiento Anti-denegación de servicios DDoS (Tipo 1) - Renovación | 2 | 2 |
| 16 | Licenciamiento Anti-denegación de servicios DDoS (Tipo 2) - Renovación | 2 | 2 |
| 17 | Redes Privadas Virtuales | 1 | 2 |
| 18 | Licenciamiento Redes Privadas Virtuales - Implementación | 1 | 2 |
| 19 | Licenciamiento Redes Privadas Virtuales - Renovación | 4 | 4 |
| 20 | Licenciamiento Filtrado de Contenido Web - Renovación | 4 | 4 |
| 21 | Licenciamiento Filtrado de Contenido de Correo (Antispam) - Renovación | 4 | 4 |
| 22 | Firewall Especializado en Servicios Web (WAF) | 1 | 2 |
| 23 | Licenciamiento Firewall Especializado en Servicios Web (WAF) - Implementación | 1 | 2 |
| 24 | Licenciamiento Firewall Especializado en Servicios Web (WAF) - Renovación | 4 | 4 |
| 25 | Firewall Especializado en Base de Datos (DBF) | 1 | 2 |
| 26 | Licenciamiento Firewall Especializado en Base de Datos (DBF) - Implementación | 1 | 2 |

| | | | |
|---|---|---|---|
| 27 | Licenciamiento Firewall Especializado en Base de Datos (DBF) - Renovación | 4 | 4 |
| 28 | Gestión Unificada de Amenazas (UTM) (Tipo 4) | 1 | 2 |
| 29 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 4) - Implementación | 1 | 2 |
| 30 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 1) - Renovación | 1 | 1 |
| 31 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 2) - Renovación | 1 | 1 |
| 32 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 3) - Renovación | 1 | 1 |
| 33 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 4) - Renovación | 1 | 1 |
| 34 | Correlación de Eventos | 2 | 4 |
| 35 | Licenciamiento Correlación de Eventos - Implementación | 2 | 4 |
| 36 | Protección de Amenazas Persistentes Avanzadas (APT) | 2 | 4 |
| 37 | Licenciamiento Protección de Amenazas Persistentes Avanzadas (APT) - Implementación | 2 | 4 |
| 38 | Borrado Seguro de Información | 1600 | 4000 |
| 39 | Ciberinteligencia | 12 | 24 |
| 40 | Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles | 3000 | 5000 |
| 41 | Gestión de control de acceso para usuarios privilegiados (AAA) | 400 | 800 |
| 42 | Sistema de Gestión de Seguridad de la Información (SGSI) | 1 | 1 |
| 43 | Gestión de Dominios | 2 | 4 |
| 44 | Certificados Digitales SSL | 16 | 20 |
| 45 | Servicios de Prevención de Perdida de Información | 80 | 200 |
| 46 | Servicio de Antivirus | 1000 | 1500 |
| 47 | Servicios de Gestión del Cambio en Seguridad de la Información | 1 | 1 |
| 48 | Servicios del Centro de Operaciones de Seguridad (SOC) | 1 | 1 |

Lo anterior de acuerdo a lo establecido en junta de aclaraciones, Precisión 3 por parte de la Convocante.

Operbes S.A. de C.V. tomó en consideración que se requiere 4 equipos Firewall tipo 3.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 1 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que las cantidades mínimas y máximas se refieren a las cantidad de discos duros/ virtuales que se deben considerar, la cantidad de equipos a borrar se encuentra relacionada con medios de almacenamientos físicos y virtuales.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 2 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración qué las cantidades mínimas y máximas se refieren a las cantidades expresadas mínima y máxima se refieren a la cantidad de agentes de Prevención de perdida de información que deberán ser considerados.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 3 de la empresa Operbes, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que para el servicio de borrado seguro de información se considera por cada evento al menos un activo a borrar.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 9 de la empresa Scitum, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que respectará los 80 y 200 agentes de los Servicios de Prevención de Perdida de Información, estos se considerarán tanto para equipo de cómputo, (laptops y PCs), así como servidores los cuales serán instalados en la localidad Morelia, Michoacán.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 1 de la empresa Silent4business, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que la solución de Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles se requiere al menos en tres inmuebles ubicados en la Ciudad de México.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 2 de la empresa Silent4business, S.A. de C.V.

Operbes S.A. de C.V. tomó en consideración que la cantidad de máxima y mínima de correlación de eventos mencionada en precisión 3 hace referencia a los dispositivos colectores.
Lo anterior de acuerdo a lo establecido en junta de aclaraciones, repregunta 3 de la empresa Silent4business, S.A. de C.V.

Atentamente

Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes
Apoderados Legales de Operbes, S.A. de C.V., actuando como Representante Común de la Participación Conjunta de las empresas Bufete Empresarial GTI, S.A. de C.V., Silent4Busines, S.A. de C.V., y Operbes, S.A. de C.V.



ANEXOS
DIVISIÓN DE CONTRATOS

# CERTIFICADOS ISO/IEC27001:2013 E ISO/IEC-20000-1:2018 VIGENTES.

# III.- PROPUESTA DE TRABAJO

# III B). - PLAN DE TRABAJO PROPUESTO POR EL LICITANTE.



ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

## PLAN DE TRABAJO.

A continuación se presenta el plan de trabajo que considerá la implemetación de los activos de infraestructura en un tiempo minimo de 30 días naturales y máximo 90 días naturales.

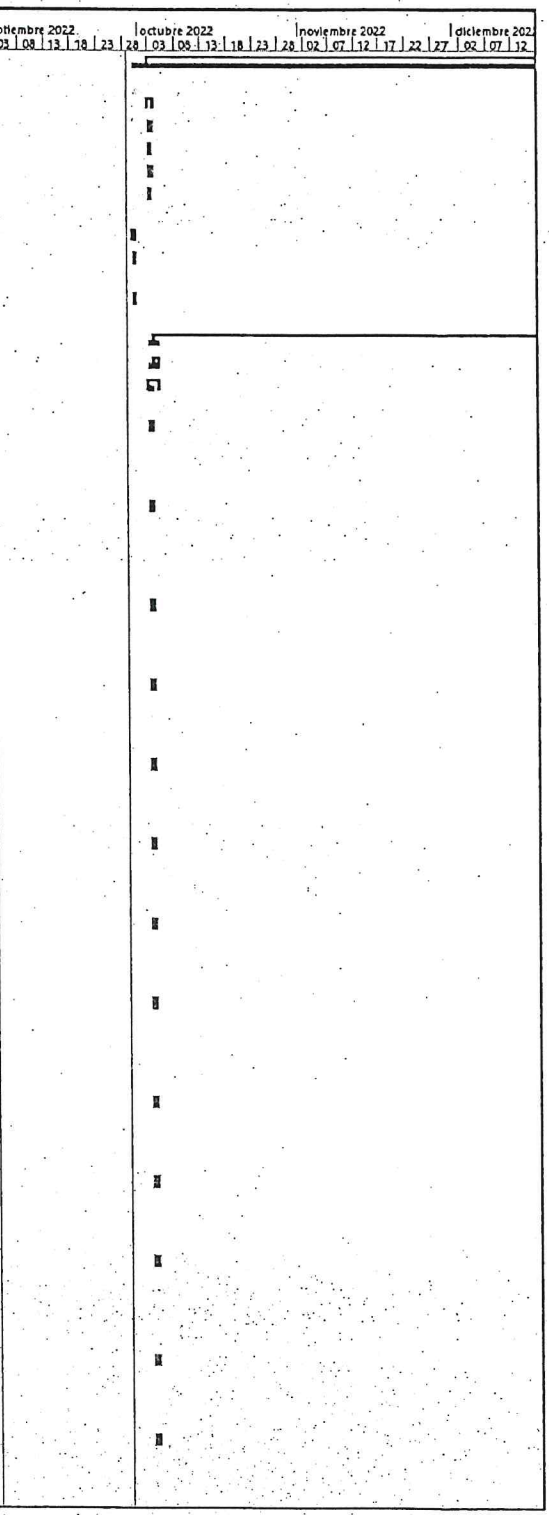
Lo anterior de acuerdo a la junta de aclaraciones, repregunta 33 de la empresa Operbes S.A. de C.V.



ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

| Id | Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin |
|---|---|---|---|---|---|
| 1 | | IMSS Servicios Administrados de Seguridad Informática (SASI) | 516 días? | lun 03/10/22 | lun 30/09/24 |
| 2 | | INICIO | 1 día | lun 03/10/22 | lun 03/10/22 |
| 3 | | Entrega de Adjudicación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 4 | | Elaboración de Alcance | 0.5 días | lun 03/10/22 | lun 03/10/22 |
| 5 | | Kick-off con el cliente | 1 día | lun 03/10/22 | lun 03/10/22 |
| 6 | | Elaboración de registro de interesados | 0.5 días | lun 03/10/22 | lun 03/10/22 |
| 7 | | PLANIFICACIÓN | 0.5 días | vie 30/09/22 | vie 30/09/22 |
| 8 | | Elaboración de plan de trabajo | 0.5 días | vie 30/09/22 | vie 30/09/22 |
| 9 | | Elaboración de plan de comunicación | 0.5 días | vie 30/09/22 | vie 30/09/22 |
| 10 | | EJECUCIÓN | 64 días? | mar 04/10/22 | vie 30/12/22 |
| 11 | | Servicios | 1 día? | mar 04/10/22 | mar 04/10/22 |
| 12 | | Renovacion de licenciamientos | 2 días? | lun 03/10/22 | mar 04/10/22 |
| 13 | | Colocacion de Orden de compra Licenciamiento Firewall (Tipo 1,2,3,4) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 14 | | Entrega de licenciamiento por fabricante para Firewall (Tipo 1,2,3,4) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 15 | | Activacion de licenciamiento para Firewall (Tipo 1,2,3,4) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 16 | | Colocacion de Orden de compra Licenciamiento IPS (Tipo 1,2,3,4) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 17 | | Entrega de licenciamiento por fabricante para IPS (Tipo 1,2,3,4) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 18 | | Activacion de licenciamiento para IPS (Tipo 1,2,3,4) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 19 | | Colocacion de Orden de compra Licenciamiento Anti DdoS (Tipo 1 y 2) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 20 | | Entrega de licenciamiento por fabricante para Anti DDoS (Tipo 1,2,3,4) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 21 | | Activacion de licenciamiento para Anti DdoS (Tipo 1 y 2) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 22 | | Colocacion de Orden de compra licenciamiento Redes Privadas Virtuales - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 23 | | Entrega de licenciamiento por fabricante para Redes Privadas Virtuales - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 24 | | Activacion de licenciamiento para Redes Privadas Virtuales - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 25 | | Colocacion de Orden de compra licenciamiento Filtrado de Contenido Web - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |



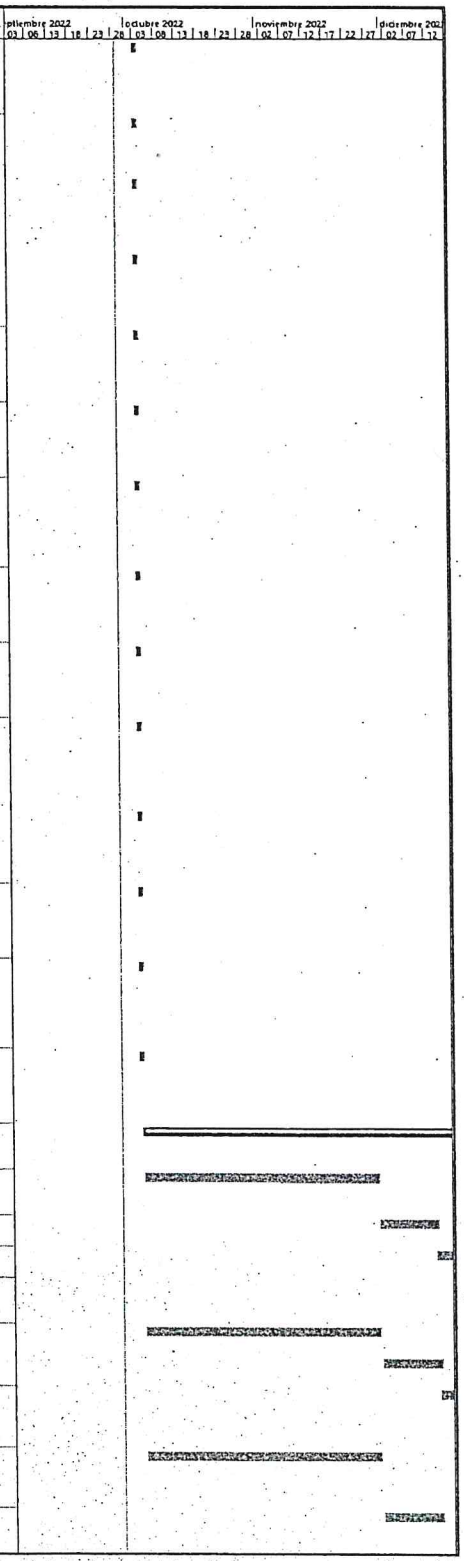



ANEXOS
DIVISIÓN DE CONTRATOS

00

SIN TEXTO

| Id | Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin |
|---|---|---|---|---|---|
| 26 | | Entrega de licenciamiento por fabricante para Filtrado de Contenido Web - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 27 | | Activacion de licenciamiento para Filtrado de Contenido Web - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 28 | | Colocacion de Orden de compra licenciamiento Filtrado de Contenido de Correo (Antispam) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 29 | | Entrega de licenciamiento por fabricante para Filtrado de Contenido de Correo (Antispam) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 30 | | Activacion de licenciamiento para Filtrado de Contenido de Correo (Antispam) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 31 | | Colocacion de Orden de compra licenciamiento Firewall Especializado en Servicios Web (WAF) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 32 | | Entrega de licenciamiento por fabricante para Firewall Especializado en Servicios Web (WAF) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 33 | | Activacion de licenciamiento para Firewall Especializado en Servicios Web (WAF) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 34 | | Colocacion de Orden de compra licenciamiento Firewall Especializado en Base de Datos (DBF) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 35 | | Entrega de licenciamiento por fabricante para Firewall Especializado en Base de Datos (DBF) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 36 | | Activacion de licenciamiento para Firewall Especializado en Base de Datos (DBF) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 37 | | Colocacion de Orden de compra licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 1,2,3 y 4) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 38 | | Entrega de licenciamiento por fabricante para Gestión Unificada de Amenazas (UTM) (Tipo 2) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 39 | | Activacion de licenciamiento para Gestión Unificada de Amenazas (UTM) (Tipo 3) - Renovación | 1 día | lun 03/10/22 | lun 03/10/22 |
| 40 | | **Implementacion de equipamiento y licenciamiento nuevo** | 65.5 días | mar 04/10/22 | sáb 31/12/22 |
| 41 | | Compra de equipo y licenciamiento Firewall (Tipo 4) | 40 días | mar 04/10/22 | lun 28/11/22 |
| 42 | | Instalacion y configuracion Firewall (Tipo 4) | 10 días | mar 29/11/22 | mar 13/12/22 |
| 43 | | Pruebas y Validaciones Firewall (Tipo 4) | 10 días | mar 13/12/22 | lun 26/12/22 |
| 44 | | Integracion al centro de operaciones SOC Firewall (Tipo 4) | 4 días | lun 26/12/22 | jue 29/12/22 |
| 45 | | Compra de equipo y licenciamiento IPS (Tipo 3) | 40 días | mar 04/10/22 | lun 28/11/22 |
| 46 | | Instalacion y configuracion IPS (Tipo 3) | 10 días | mar 29/11/22 | mar 13/12/22 |
| 47 | | Pruebas y Validaciones IPS (Tipo 3) | 10 días | mar 13/12/22 | lun 26/12/22 |
| 48 | | Integracion al centro de operaciones SOC IPS (Tipo | 4 días | lun 26/12/22 | jue 29/12/22 |
| 49 | | Compra de equipo y licenciamiento Anti-denegación de servicios DDoS (Tipo 2) | 40 días | mar 04/10/22 | lun 28/11/22 |
| 50 | | Instalacion y configuracion Anti-denegación de servicios DDoS (Tipo 2) | 10 días | mar 29/11/22 | mar 13/12/22 |

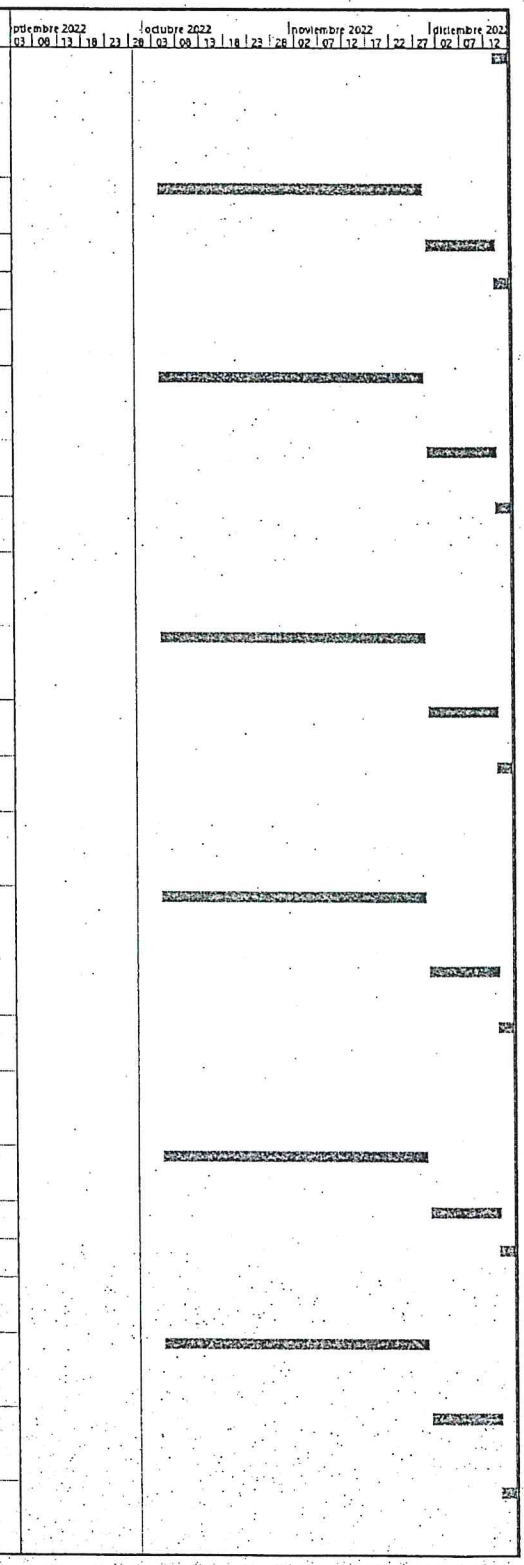





ANEXOS
DIVISIÓN DE

SIN TEXTO

| Id | Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin |
|---|---|---|---|---|---|
| 51 | | Pruebas y Validaciones Anti-denegación de servicios DDoS (Tipo 2) | 10 días | mar 13/12/22 | lun 26/12/22 |
| 52 | | Integracion al centro de operaciones SOC Anti-denegación de servicios DDoS (Tipo 2) | 4 días | lun 26/12/22 | jue 29/12/22 |
| 53 | | Compra de equipo y licenciamiento Redes Privadas Virtuales | 40 días | mar 04/10/22 | lun 28/11/22 |
| 54 | | Instalacion y configuracion Redes Privadas Virtuales | 10 días | mar 29/11/22 | mar 13/12/22 |
| 55 | | Pruebas y Validaciones Redes Privadas Virtuales | 10 días | mar 13/12/22 | lun 26/12/22 |
| 56 | | Integracion al centro de operaciones SOC Redes Privadas Virtuales | 4 días | lun 26/12/22 | jue 29/12/22 |
| 57 | | Compra de equipo y licenciamiento Firewall Especializado en Servicios Web (WAF) | 40 días | mar 04/10/22 | lun 28/11/22 |
| 58 | | Instalacion y configuracion Firewall Especializado en Servicios Web (WAF) | 10 días | mar 29/11/22 | mar 13/12/22 |
| 59 | | Pruebas y Validaciones Firewall Especializado en Servicios Web (WAF) | 10 días | mar 13/12/22 | lun 26/12/22 |
| 60 | | Integracion al centro de operaciones SOC Firewall Especializado en Servicios Web (WAF) | 4 días | lun 26/12/22 | jue 29/12/22 |
| 61 | | Compra de equipo y licenciamiento Firewall Especializado en Base de Datos (DBF) | 40 días | mar 04/10/22 | lun 28/11/22 |
| 62 | | Instalacion y configuracion Firewall Especializado en Base de Datos (DBF) | 10 días | mar 29/11/22 | mar 13/12/22 |
| 63 | | Pruebas y Validaciones Firewall Especializado en Base de Datos (DBF) | 10 días | mar 13/12/22 | lun 26/12/22 |
| 64 | | Integracion al centro de operaciones SOC Firewall Especializado en Base de Datos (DBF) | 4 días | lun 26/12/22 | jue 29/12/22 |
| 65 | | Compra de equipo y licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 4) | 40 días | mar 04/10/22 | lun 28/11/22 |
| 66 | | Instalacion y configuracion Gestión Unificada de Amenazas (UTM) (Tipo 4) | 10 días | mar 29/11/22 | mar 13/12/22 |
| 67 | | Pruebas y Validaciones Gestión Unificada de Amenazas (UTM) (Tipo 4) | 10 días | mar 13/12/22 | lun 26/12/22 |
| 68 | | Integracion al centro de operaciones SOC Gestión Unificada de Amenazas (UTM) (Tipo 4) | 4 días | lun 26/12/22 | jue 29/12/22 |
| 69 | | Compra de equipo y licenciamiento Correlación de Eventos | 40 días | mar 04/10/22 | lun 28/11/22 |
| 70 | | Instalacion y configuracion Correlación de Eventos | 10 días | mar 29/11/22 | mar 13/12/22 |
| 71 | | Pruebas y Validaciones Correlación de Eventos | 10 días | mar 13/12/22 | lun 26/12/22 |
| 72 | | Integracion al centro de operaciones SOC Correlación de Eventos | 4 días | lun 26/12/22 | jue 29/12/22 |
| 73 | | Compra de equipo y licenciamiento Protección de Amenazas Persistentes Avanzadas (APT) | 40 días | mar 04/10/22 | lun 28/11/22 |
| 74 | | Instalacion y configuracion Protección de Amenazas Persistentes Avanzadas (APT) | 10 días | mar 29/11/22 | mar 13/12/22 |
| 75 | | Pruebas y Validaciones Protección de Amenazas Persistentes Avanzadas (APT) | 10 días | mar 13/12/22 | lun 26/12/22 |






ANEXOS
REVISIÓN DE CONTRATOS

SIN TEXTO

| Id | Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin |
|---|---|---|---|---|---|
| 76 | | Integracion al centro de operaciones SOC Protección de Amenazas Persistentes Avanzadas | 4 días | lun 26/12/22 | jue 29/12/22 |
| 77 | | Compra de servicio de Borrado Seguro de Información | 30 días | mar 04/10/22 | mar 15/11/22 |
| 78 | | Aplicación del servicio de Borrado Seguro de Información *Bajo | 34 días | mar 15/11/22 | jue 29/12/22 |
| 79 | | Pruebas de aplicaciones Borrado Seguro de Información | 2 días | jue 29/12/22 | vie 30/12/22 |
| 80 | | Suministro de servicio de Ciberinteligencia | 30 días | mar 04/10/22 | mar 15/11/22 |
| 81 | | Integracion al centro de operaciones SOC Ciberintelligencia | 2 días | mar 15/11/22 | mié 16/11/22 |
| 82 | | Compra de equipo y licenciamiento Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles | 40 días | mar 04/10/22 | lun 28/11/22 |
| 83 | | Instalacion y configuracion Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles | 10 días | mar 29/11/22 | mar 13/12/22 |
| 84 | | Pruebas y Validaciones Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles | 10 días | mar 13/12/22 | lun 26/12/22 |
| 85 | | Integracion al centro de operaciones SOC Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles | 4 días | lun 26/12/22 | jue 29/12/22 |
| 86 | | Compra de equipo y licenciamiento Gestión de control de acceso para usuarios privilegiados | 40 días | mar 04/10/22 | lun 28/11/22 |
| 87 | | Instalacion y configuracion Gestión de control de acceso para usuarios privilegiados (AAA) | 10 días | mar 29/11/22 | mar 13/12/22 |
| 88 | | Pruebas y Validaciones Gestión de control de acceso para usuarios privilegiados (AAA) | 10 días | mar 13/12/22 | lun 26/12/22 |
| 89 | | Integracion al centro de operaciones SOC Gestión de control de acceso para usuarios privilegiados | 4 días | lun 26/12/22 | jue 29/12/22 |
| 90 | | Suministro de Sistema de Gestión de Seguridad de la Información (SGSI) | 30 días | mar 04/10/22 | mar 15/11/22 |
| 91 | | Compra de servicio de Gestión de Dominios | 30 días | mar 04/10/22 | mar 15/11/22 |
| 92 | | Aplicación de servicio Gestión de Dominios | 1 día | mar 15/11/22 | mar 15/11/22 |
| 93 | | Compra de servicio Certificados Digitales SSL | 30 días | mar 04/10/22 | mar 15/11/22 |
| 94 | | Aplicación de servicio de Certificados Digitales SSL | 1 día | mar 15/11/22 | mar 15/11/22 |
| 95 | | Compra de equipo y licenciamiento Servicios de Prevención de Perdida de Información | 40 días | mar 04/10/22 | lun 28/11/22 |
| 96 | | Instalacion y configuracion Servidos de Prevención de Perdida de Información | 10 días | mar 29/11/22 | mar 13/12/22 |
| 97 | | Pruebas y Validaciones Servidos de Prevención de Perdida de Información | 10 días | mar 13/12/22 | lun 26/12/22 |
| 98 | | Integracion al centro de operaciones SOC Servidos de Prevención de Perdida de Información | 4 días | lun 26/12/22 | jue 29/12/22 |
| 99 | | Compra de licencias de Servicio de Antivirus | 30 días | mar 04/10/22 | mar 15/11/22 |
| 100 | | Instalacion y configuracion de licencia de Servicio de Antivirus | 10 días | mar 15/11/22 | sáb 26/11/22 |

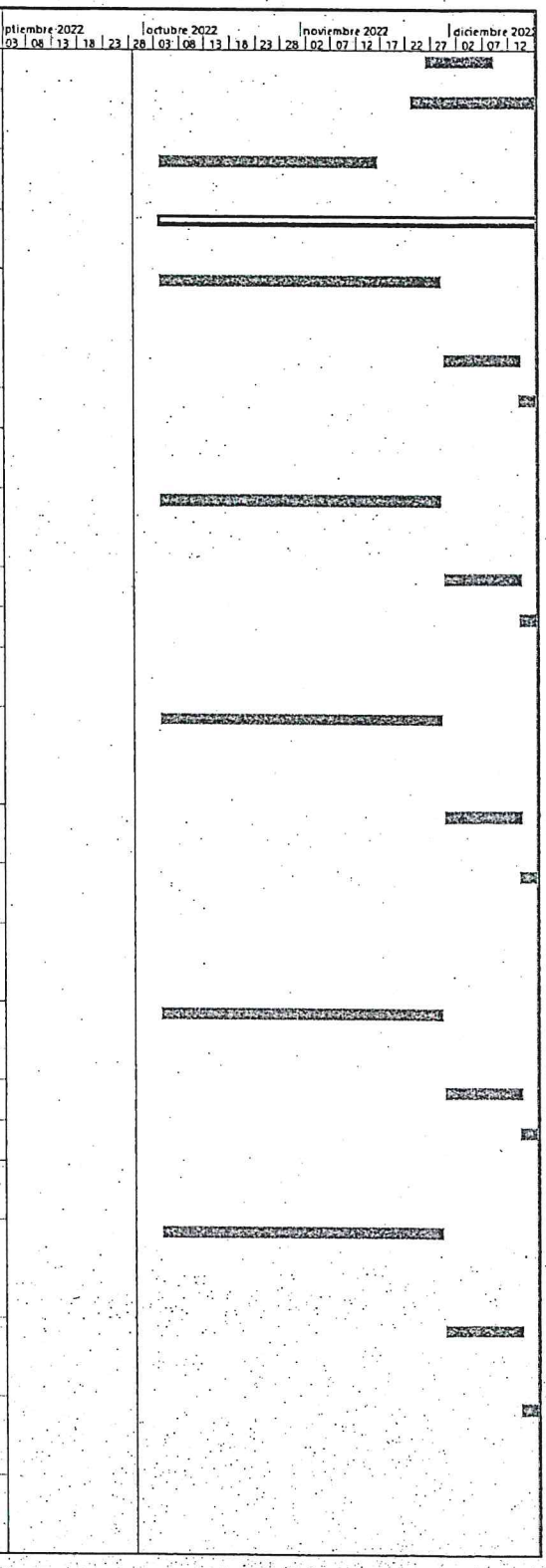




ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

| Id. | Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin |
|---|---|---|---|---|---|
| 101 | | Pruebas y Validaciones Servido de Antivirus | 10 días | sáb 26/11/22 | jue 08/12/22 |
| 102 | | Suministro de Servicios de Gestión del Cambio en Seguridad de la | 30 días | mar 22/11/22 | sáb 31/12/22 |
| 103 | | Suministro de servicios del Centro de Operaciones de seguridad (SOC) | 30 días | mar 04/10/22 | mar 15/11/22 |
| 104 | | **Cambios de solucion de la Infraestructura existente a equipamiento nuevo** | 65 días? | mar 04/10/22 | sáb 31/12/22 |
| 105 | | Colocacion de Orden de compra de equipamiento y Licenciamiento Firewall (Tipo 1,2,3,4) | 40 días | mar 04/10/22 | lun 28/11/22 |
| 106 | | Instalacion y configuracion para Firewall (Tipo 1,2,3,4) | 10 días | mar 29/11/22 | mar 13/12/22 |
| 107 | | Pruebas y Validaciones Firewall (Tipo 1,2,3,4) | 10 días | mar 13/12/22 | lun 26/12/22 |
| 108 | | Integracion al centro de operaciones SOC Firewall (Tipo 1,2,3,4) | 4 días | lun 26/12/22 | jue 29/12/22 |
| 109 | | Colocacion de Orden de compra de equipamiento y Licenciamiento IPS (Tipo 1,2,3,4) | 40 días | mar 04/10/22 | lun 28/11/22 |
| 110 | | Instalacion y configuracion para IPS (Tipo 1,2,3,4) | 10 días | mar 29/11/22 | mar 13/12/22 |
| 111 | | Pruebas y Validaciones IPS (Tipo 1,2,3,4) | 10 días | mar 13/12/22 | lun 26/12/22 |
| 112 | | Integracion al centro de operaciones SOC IPS (Tipo 1,2,3,4) | 4 días | lun 26/12/22 | jue 29/12/22 |
| 113 | | Colocacion de Orden de compra de equipamiento y Licenciamiento Anti-denegación de servicios DDoS (Tipo 1 y 2) | 40 días | mar 04/10/22 | lun 28/11/22 |
| 114 | | Instalacion y configuracion para Anti-denegación de servicios DDoS (Tipo 1 y 2) | 10 días | mar 29/11/22 | mar 13/12/22 |
| 115 | | Pruebas y Validaciones Anti-denegación de servicios DDoS (Tipo 1 y 2) | 10 días | mar 13/12/22 | lun 26/12/22 |
| 116 | | Integracion al centro de operaciones SOC Anti-denegación de servicios DDoS (Tipo 1 y 2) | 4 días | lun 26/12/22 | jue 29/12/22 |
| 117 | | Colocacion de Orden de compra de equipamiento y Licenciamiento Redes Privadas Virtuales | 40 días | mar 04/10/22 | lun 28/11/22 |
| 118 | | Instalacion y configuracion para Redes Privadas | 10 días | mar 29/11/22 | mar 13/12/22 |
| 119 | | Pruebas y Validaciones Redes Privadas Virtuales | 10 días | mar 13/12/22 | lun 26/12/22 |
| 120 | | Integracion al centro de operaciones SOC Redes Privadas Virtuales | 4 días | lun 26/12/22 | jue 29/12/22 |
| 121 | | Colocacion de Orden de compra de equipamiento y Licenciamiento Gestión Unificada de Amenazas (UTM) Tipo 1, 2, 3 y 4 | 40 días | mar 04/10/22 | lun 28/11/22 |
| 122 | | Instalacion y configuracion para Gestión Unificada de Amenazas (UTM) Tipo 1, 2, 3 y 4 | 10 días | mar 29/11/22 | mar 13/12/22 |
| 123 | | Pruebas y Validaciones Gestión Unificada de Amenazas (UTM) Tipo 1, 2, 3 y 4 | 10 días | mar 13/12/22 | lun 26/12/22 |
| 124 | | Integracion al centro de operaciones SOC Gestión Unificada de Amenazas (UTM) Tipo 1, 2, 3 y 4 | 4 días | lun 26/12/22 | jue 29/12/22 |

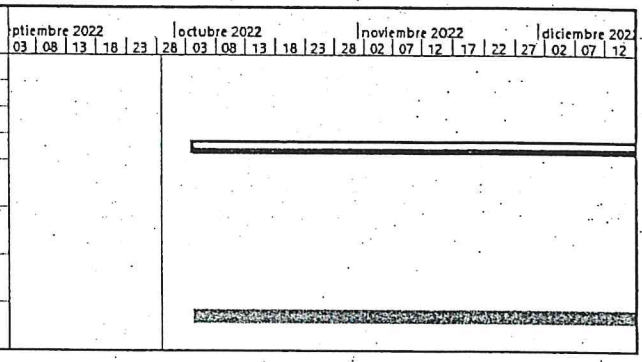





ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

| Id | Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin |
|---|---|---|---|---|---|
| 125 | | MONITOREO Y CONTROL | 20 días | sáb 31/12/22 | vie 27/01/23 |
| 126 | | Reuniones Semanales 1 | 0.5 días | sáb 31/12/22 | sáb 31/12/22 |
| 131 | | Reuniones Semanales 2 | 0.5 días | sáb 31/12/22 | sáb 31/12/22 |
| 136 | | CIERRE | 515 días | mar 04/10/22 | lun 30/09/24 |
| 137 | | Elaboración de Memoria Técnica | 1 día | sáb 31/12/22 | lun 02/01/23 |
| 138 | | Entrega de carta de entrega de sitio (CIOA) | 1 día | sáb 31/12/22 | lun 02/01/23 |
| 139 | | Entrega Completa de servicios SOC | 2 días | sáb 31/12/22 | mar 03/01/23 |
| 140 | | Operación de servicios de seguridad IMSS | 515 días | mar 04/10/22 | lun 30/09/24 |






ANEXOS
ENVIADOS DE CONTRATOS

SIN TEXTO

**III b). - Plan de trabajo propuesto por el licitante**
**Manifiesto inciso B**

Ciudad de México, a 30 de septiembre de 2022.

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

**Procedimiento Número:** LA-050GYR019-E182-2022

Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes, en nuestro carácter de representantes legales de la empresa Operbes, S.A. de C.V., actuando como representante común de la participación conjunta de las empresas Silent4Business, S.A. de C.V., Bufete Empresarial GTI, S.A. de C.V., y Operbes, S.A. de C.V., manifestamos bajo protesta de decir verdad, que garantizamos el cumplimiento de la totalidad de las características técnicas de la oferta de nuestra representada, alineada a los apartados y requerimientos establecidos en el Anexo Técnico y los Términos y Condiciones.

Protestamos lo necesario

Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes
Apoderados Legales de Operbes, S.A. de C.V., actuando como Representante Común de la Participación Conjunta de las empresas Bufete Empresarial GTI, S.A. de C.V., Silent4Busines, S.A. de C.V., y Operbes, S.A. de C.V.



ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

## Anexo 9- Propuesta Económica

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

| PARTIDA 1 | | | |
|---|---|---|---|
| **No.** | **Descripción de Servicio** | **Unidad de Medida** | **Precio Unitario** |
| 1 | Firewall (Tipo 4) | Servicio | $ 1,785,781.00 |
| 2 | Licenciamiento Firewall (Tipo 4) - Implementación | Servicio | $ 123,766.00 |
| 3 | Licenciamiento Firewall (Tipo 1) - Renovación | Servicio | $ 260,780.00 |
| 4 | Licenciamiento Firewall (Tipo 2) - Renovación | Servicio | $ 290,791.00 |
| 5 | Licenciamiento Firewall (Tipo 3) - Renovación | Servicio | $ 432,299.00 |
| 6 | Licenciamiento Firewall (Tipo 4) - Renovación | Servicio | $ 2,641,549.00 |
| 7 | IPS (Tipo 3) | Servicio | $ 1,325,217.00 |
| 8 | Licenciamiento IPS (Tipo 3 ) - Implementación | Servicio | $ 91,846.00 |
| 9 | Licenciamiento IPS (Tipo 1) - Renovación | Servicio | $ 1,385,131.00 |
| 10 | Licenciamiento IPS (Tipo 2) - Renovación | Servicio | $ 2,579,102.00 |
| 11 | Licenciamiento IPS (Tipo 3) - Renovación | Servicio | $ 2,783,010.00 |
| 12 | Licenciamiento IPS (Tipo 4) - Renovación | Servicio | $ 2,783,010.00 |
| 13 | Anti-denegación de servicios DDoS (Tipo 2) | Servicio | $ 1,405,244.00 |
| 14 | Licenciamiento Anti-denegación de servicios DDoS (Tipo 2) - Implementación | Servicio | $ 111,642.00 |
| 15 | Licenciamiento Anti-denegación de servicios DDoS (Tipo 1) - Renovación | Servicio | $ 4,128,555.00 |
| 16 | Licenciamiento Anti-denegación de servicios DDoS (Tipo 2) - Renovación | Servicio | $ 4,128,555.00 |
| 17 | Redes Privadas Virtuales | Servicio | $ 38,467.00 |
| 18 | Licenciamiento Redes Privadas Virtuales - Implementación | Servicio | $ 5,332.00 |
| 19 | Licenciamiento Redes Privadas Virtuales - Renovación | Servicio | $ 86,024.00 |
| 20 | Licenciamiento Filtrado de Contenido Web - Renovación | Servicio | $ 1,477,582.00 |
| 21 | Licenciamiento Filtrado de Contenido de Correo (Antispam) - Renovación | Servicio | $ 2,234,468.00 |
| 22 | Firewall Especializado en Servicios Web (WAF) | Servicio | $ 4,661,810.00 |
| 23 | Licenciamiento Firewall Especializado en Servicios Web (WAF) - Implementación | Servicio | $ 776,141.00 |
| 24 | Licenciamiento Firewall Especializado en Servicios Web (WAF) - Renovación | Servicio | $ 7,634,198.00 |
| 25 | Firewall Especializado en Base de Datos (DBF) | Servicio | $ 6,130,449.00 |
| 26 | Licenciamiento Firewall Especializado en Base de Datos (DBF) - Implementación | Servicio | $ 776,141.00 |
| 27 | Licenciamiento Firewall Especializado en Base de Datos (DBF) - Renovación | Servicio | $ 2,804,935.00 |
| 28 | Gestión Unificada de Amenazas (UTM) (Tipo 4) | Servicio | $ 70,565.00 |
| 29 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 4) - Implementación | Servicio | $ 4,891.00 |
| 30 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 1) - Renovación | Servicio | $ 32,403.00 |



ANEXOS
DIVISIÓN DE CONTRATOS

| | | | | |
|---|---|---|---|---|
| 31 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 2) - Renovación | Servicio | $ | 48,483.00 |
| 32 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 3) - Renovación | Servicio | $ | 139,542.00 |
| 33 | Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 4) - Renovación | Servicio | $ | 271,537.00 |
| 34 | Correlación de Eventos | Servicio | $ | 2,938,566.00 |
| 35 | Licenciamiento Correlación de Eventos - Implementación | Servicio | $ | 397,765.00 |
| 36 | Protección de Amenazas Persistentes Avanzadas (APT) | Servicio | $ | 4,948,128.00 |
| 37 | Licenciamiento Protección de Amenazas Persistentes Avanzadas (APT) - Implementación | Servicio | $ | 355,868.00 |
| 38 | Borrado Seguro de Información | Servicio | $ | 650.00 |
| 39 | Ciberinteligencia | Servicio | $ | 525,629.00 |
| 40 | Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles | Servicio | $ | 9,472.00 |
| 41 | Gestión de control de acceso para usuarios privilegiados (AAA) | Servicio | $ | 18,031.00 |
| 42 | Sistema de Gestión de Seguridad de la Información (SGSI) | Servicio | $ | 590,910.00 |
| 43 | Gestión de Dominios | Servicio | $ | 71,591.00 |
| 44 | Certificados Digitales SSL | Servicio | $ | 47,489.00 |
| 45 | Servicios de Prevención de Perdida de Información | Servicio | $ | 12,072.00 |
| 46 | Servicio de Antivirus | Servicio | $ | 6,372.00 |
| 47 | Servicios de Gestión del Cambio en Seguridad de la Información | Servicio | $ | 545,455.00 |
| 48 | Servicios del Centro de Operaciones de Seguridad (SOC) | Servicio | $ | 28,740,623.00 |
| | **Suma de Precios Unitarios:** | | $ | 92,657,867.00 |

Monto en letra sin IVA ( Noventa y dos millones seiscientos cincuenta y siete mil ochocientos sesenta y siete pesos 00/100 M.N.)

Precios serán fijos durante la vigencia del contrato
Los servicios objeto de esta licitación se cotizan en pesos mexicanos

**Razón Social.- Operbes, S.A. de C.V., actuando como Representante Común de la Participación Conjunta de las empresas Bufete Empresarial GTI, S.A. de C.V., Silent4Busines, S.A. de C.V., y Operbes, S.A. de C.V**
**RFC.- OPE070326DNA**
**Lugar y fecha.- Ciudad de México, a 30 de septiembre de 2022**

Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes
Apoderados Legales de Operbes, S.A. de C.V., actuando como Representante Común de la Participación Conjunta de las empresas Bufete Empresarial GTI, S.A. de C.V., Silent4Busines, S.A. de C.V., y Operbes, S.A. de C.V.

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-E182-2022
OBJETO DE LA LICITACIÓN: SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024.

En la Ciudad de México, siendo las **11:00 horas del día 04 de octubre de 2022**, en la **Sala 5, del Sótano Ala Poniente del edificio de Avenida Paseo de la Reforma No. 476, Colonia Juárez, C.P. 06600, Demarcación Territorial Cuauhtémoc**, se reunieron los servidores públicos cuyos nombres y firmas aparecen al final de la presente Acta con el objeto de llevar a cabo el Acto de Notificación del Fallo de la Licitación Pública Nacional Electrónica, con número de identificación en CompraNet **LA-050GYR019-E182-2022**, convocada para la contratación de los **"Servicios Administrados de Seguridad Informática (SASI) 2022-2024"**, de conformidad con el artículo 37 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante, la Ley o la LAASSP), así como lo previsto en el apartado 3, **numeral 3.11, inciso a)** de la Convocatoria: ----------

---

Este acto es presidido por la Maestra Elia Sandra Varas Galeana, 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, de conformidad 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 7.1.3.1.2.3, del Manual de Organización de la Dirección de Administración, quien rubrica y firma al final de la presente acta. ----------

---

Quien preside el acto hace del conocimiento que el presente evento está siendo videograbado, de conformidad con lo dispuesto en los numerales 6 y 8 de la sección II del "Acuerdo por el cual se expide el protocolo de actuación en materia de contrataciones públicas, otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones", publicado en el Diario Oficial de la Federación el 20 de agosto de 2015; con relación al Transitorio Segundo fracción II del "Acuerdo por el que se modifica el diverso que expide el protocolo de actuación en materia de contrataciones públicas, otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones", publicado en el Diario Oficial de la Federación el 19 de febrero de 2016, así como el "Acuerdo por el que se modifica el diverso que expide el protocolo de actuación en materia de contrataciones públicas, otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones", publicado en el Diario Oficial de la Federación el 28 de febrero de 2017. ----------

---

Se hace constar que se encuentra presente el Titular de la División de Seguridad Informática Física, con carácter de Área Requirente y Técnica, cuyo nombre y firma aparecen al final de la presente Acta.

---

Asimismo, se hace constar que se encuentran presentes los representantes del Órgano Interno de Control en el Instituto y de la Coordinación de Legislación y Consulta, cuyos nombres y firmas aparecen al final del Acta.----------

---

De conformidad con los artículos 26 penúltimo párrafo de la LAASSP y 45 de su Reglamento, se hace constar que no asistieron personas que hayan manifestado su interés de estar presentes en este acto como observadores. ----------

---

Acto seguido, en presencia de los asistentes se da lectura al contenido en la presente acta, al tenor de lo siguiente: ----------

---

En el acto de presentación y apertura de proposiciones, se recibió para efectos de su revisión, análisis detallado y elaboración del Dictamen que fundamenta y motiva el Fallo de la presente Licitación, conforme lo establecen los artículos 36 y 36 Bis fracción I de la Ley, 51 primer párrafo, así como 52 del Reglamento, las proposiciones de los siguientes licitantes: ----------

---

---

ANEXOS
DIVISIÓN DE CONTRATOS

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-E182-2022
OBJETO DE LA LICITACIÓN: SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024.

| No. | Licitante | Partida en la que Participa |
|---|---|---|
| 1 | Totalsec, S.A. de C.V. en participación conjunta con Total Play Telecomunicaciones, SAPI de C.V. | 1 |
| 2 | Operbes, S.A. de C.V., en participación conjunta con Silent4Bussines, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V. | 1 |
| 3 | Axtel, S.A.B. de C.V. | 2 |
| 4 | Consulting All Service In Telecom And Medice S. de R.L. de C.V., en participación conjunta con Bohmer Strategists, S. de R.L. de C.V. y Secure Labs, S.A. de C.V. | 2 |
| 5 | Mnemo Evolution & Integration Services México, S.A. de C.V., en participación conjunta con Software Express S.A de C. V. | 2 |
| 6 | PG Ranhtoe Servicios Administrativos, S.A. de C.V. | 2 |
| 7 | Scitum S.A. de C.V. | 2 |
| 8 | Sixsigma Networks México, S.A. de C.V. en participación conjunta con SM4RT Security Services, S.A. de C.V. y B Drive It, S.A. de C.V. | 2 |

Se comunica a los licitantes que se verificó el **Directorio de Proveedores y Contratistas Sancionados** disponible en: https://directoriosancionados.funcionpublica.gob.mx/SanFicTec/jsp/Ficha_Tecnica/SancionadosN.htm, con corte al 05 de octubre de 2022, así como el listado de las personas impedidas para contratar con el IMSS, conforme a lo dispuesto en los artículos 50 y 60 de "La Ley" y 88 del "Reglamento", con corte al 05 de octubre de 2022. De dicha verificación se constató que los licitantes participantes en el presente procedimiento no se encuentran en dichos listados; los directorios se imprimieron y serán integrados en el expediente de la presente contratación.----------

**Criterio de Evaluación de Proposiciones** ----------

Con apego en lo dispuesto por los artículos 36 y 36 Bis fracción I de la Ley, 51 primer párrafo y 52 del Reglamento; el Capítulo Segundo, Sección Cuarta en su Décimo Lineamiento, del Acuerdo por el que se emiten diversos Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios y de Obras Públicas y Servicios Relacionados con las Mismas, publicado en el Diario Oficial de la Federación el 9 de septiembre de 2010; el Criterio TU-01/2012 emitido por la Secretaría de la Función Pública el 9 de enero de 2012; la evaluación de las proposiciones se realizó utilizando el criterio de puntos, considerando exclusivamente los requisitos y condiciones establecidos en la Convocatoria, en el Anexo Uno "Anexo Técnico", Dos "Términos y Condiciones y Nueve "Propuesta Económica", a efecto de que se garantice satisfactoriamente el cumplimiento de las obligaciones respectivas numeral 2.7 Forma de Adjudicación y Apartado 6. Criterios específicos conforme a los cuales se evaluará la proposición, ambos de la Convocatoria; así como el numeral, 7 Adjudicación de Contrato. ----------

Para tal efecto, se llevará a cabo la evaluación de la proposición del licitante, conforme al siguiente procedimiento:----------

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-E182-2022
OBJETO DE LA LICITACIÓN: SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024.

## I. EVALUACIÓN DE LAS PROPOSICIONES.

### A. FIRMA ELECTRÓNICA.

En primer término, se verificó si la proposición fue debidamente firmada electrónicamente, tal como se exigió en el apartado 3, numeral 3.3 de la Convocatoria y de conformidad con los artículos 26 Bis, fracción II y 27 de la Ley, que disponen que en el caso de Licitaciones Públicas Electrónicas, en las cuales se permite exclusivamente la participación de los licitantes a través del Sistema CompraNet, se utilizarán medios de identificación electrónica, los cuales producirán los mismos efectos que las leyes otorguen a los documentos firmados autógrafamente y, en consecuencia, tendrán el mismo valor probatorio.

Vinculado a ello, el artículo 50 del Reglamento, establece que "En las proposiciones enviadas a través de medios remotos de comunicación electrónica, en sustitución de la firma autógrafa, se emplearán medios de identificación electrónica que establezca la Secretaría de la Función Pública". Al respecto, la Secretaría de la Función Pública, mediante el "Acuerdo por el que se establecen las disposiciones que se deberán observar para la utilización del Sistema Electrónico de Información Pública Gubernamental denominado CompraNet", publicado en el Diario Oficial de la Federación el 28 de junio de 2011, dispuso en su numeral 14 textualmente lo siguiente: "El medio de identificación electrónica para que los potenciales licitantes nacionales, ya sean personas físicas o morales, hagan uso de CompraNet, será el certificado digital de la firma electrónica avanzada que emite el Servicio de Administración Tributaria para el cumplimiento de obligaciones fiscales".

Al efectuar el acto de presentación y apertura de las proposiciones, se imprimió del licitante, entre otras constancias, la relativa a la "Información General del Archivo"; "Parámetros Técnicos – PROPUESTA TÉCNICA" y "Parámetros Económicos – PROPUESTA ECONÓMICA", en razón de que los requerimientos técnicos y económicos firmados digitalmente, se identifican en el Sistema CompraNet con la denominación "TechnicalEnvelopeSummary.pdf.p7m" y "PriceEnvelopeSummary.pdf.p7m", respectivamente, y son "la prueba" de que las propuestas las autentican los licitantes como enviadas por ellos mismos a través de los medios electrónicos y, por tanto, ponen de manifiesto que la propuesta fue firmada digitalmente y que se cumplió con la exigencia prevista en la Convocatoria.

El análisis a que se refiere este numeral, se realizó por el área contratante, la División de Contratación de Activos y Logística adscrita a la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos, de la Coordinación de Adquisición de Bienes y Contratación de Servicios.

De la evaluación realizada, se desprende que los reportes arrojados por el Sistema CompraNet indican que tanto la propuesta técnica como la económica que presentaron los licitantes: **1)** Totalsec, S.A. de C.V. en participación conjunta con Total Play Telecomunicaciones, SAPI de C.V., **2)** Operbes, S.A. de C.V., en participación conjunta con Silent4Bussines, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V., **3)** Axtel, S.A.B. de C.V., **4)** Consulting All Service In Telecom And Medice S. de R.L. de C.V., en participación conjunta con Bohmer Strategists, S. de R.L. de C.V. y Secure Labs, S.A. de C.V., **5)** Mnemo Evolution & Integration Services México, S.A. de C.V., en participación conjunta con Software Express S.A de C. V., **6)** PG Ranhtoe Servicios Administrativos, S.A. de C.V., **7)** Scitum S.A. de C.V. y **8)** Sixsigma Networks México, S.A. de C.V. en participación conjunta con SM4RT Security Services, S.A. de C.V. y B Drive It, S.A. de C.V. ; **fueron debidamente firmadas en forma electrónica** con un Certificado Digital "Válido".



ANEXOS
DIVISIÓN DE CONTRATOS

ACTA DE FALLO
LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-E182-2022
OBJETO DE LA LICITACIÓN: SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024.

---

**B. EVALUACIÓN DE LA DOCUMENTACIÓN DISTINTA A LA PROPOSICIÓN (LEGAL-ADMINISTRATIVA).** ----------

Sólo después de constatar que los licitantes firmaron adecuadamente su proposición, se procedió a la evaluación de la documentación distinta a la proposición a que se refiere el apartado 4. REQUISITOS QUE LOS LICITANTES DEBEN CUMPLIR, numeral 4.2. Documentación distinta a la proposición (legal-administrativa), de la Convocatoria. ----------

La revisión de la documentación distinta a la proposición, se realizó por el área contratante, 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, de conformidad con el numeral 4.39 primer párrafo de las POBALINES, así como del numeral 4.2.2.1.15 del Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante el Manual). ----------

La evaluación se contiene en el **Anexo I,** la cual se tiene por reproducida en este apartado como si a la letra se insertare.----------

Con base en la evaluación, se concluyó que la documentación distinta que presentaron los licitantes: **1)** Totalsec, S.A. de C.V. en participación conjunta con Total Play Telecomunicaciones, SAPI de C.V., **2)** Operbes, S.A. de C.V., en participación conjunta con Silent4Bussines, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V., **3)** Axtel, S.A.B. de C.V., **4)** Consulting All Service In Telecom And Medice S. de R.L. de C.V., en participación conjunta con Bohmer Strategists, S. de R.L. de C.V. y Secure Labs, S.A. de C.V., **5)** Mnemo Evolution & Integration Services México, S.A. de C.V., en participación conjunta con Software Express S.A de C. V., **6)** PG Ranhtoe Servicios Administrativos, S.A. de C.V., **7)** Scitum S.A. de C.V. y **8)** Sixsigma Networks México, S.A. de C.V. en participación conjunta con SM4RT Security Services, S.A. de C.V. y B Drive It, S.A. de C.V.; **cumplen satisfactoriamente** con los extremos solicitados en la Convocatoria. ----------

**C. EVALUACIÓN DE LAS PROPUESTAS TÉCNICAS.** ----------

Una vez que se verificó que los licitantes cumplieron con el requerimiento de la documentación distinta, se procedió a la evaluación de los requisitos establecidos en el numeral 4. Requisitos que los licitantes deben cumplir numeral 4.1 Firma electrónica, 4.3.- Propuesta Técnica, 4.4 Propuesta económica y en el Anexo 1.- "Anexo Técnico", todos de la convocatoria, considerando el resultado de la Junta de Aclaraciones respectiva ----------

La evaluación de las propuestas técnicas de los licitantes se realizó bajo la más estricta responsabilidad del Área Técnica por parte del Ing. Abraham Gutiérrez Castillo, Titular de la División de Seguridad Informática Física, de conformidad con el artículo 2, fracciones II y III del Reglamento; los numerales 4.25, inciso e) y 4.39 primer párrafo de las POBALINES, así como del numeral 4.2.2.1.16 del Manual, remitida mediante oficio número 09 52 76 61 5A01/0114/2022 que contiene las razones del Área Requirente y Técnica, misma que se contiene en el **Anexo II**, y se tiene por reproducido en este apartado como si a la letra se insertare. ----------

Del análisis efectuado a las propuestas técnicas de los licitantes, se desprende lo siguiente: ----------

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-E182-2022
OBJETO DE LA LICITACIÓN: SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024.

Se procedió a la asignación de los 60 puntos determinados para la propuesta técnica. considerando para tal efecto la acreditación documental que, en su caso, hayan realizado los licitantes de los rubros y subrubros que integran la Matriz de Puntos y los parámetros dispuestos en cada uno de ellos, por lo que sólo se asignó el total de la puntuación a que se refiere cada rubro y subrubro, cuando los licitantes hayan acreditado los extremos y parámetros exigidos en cada uno de ellos; a partir del número mínimo y hasta el número máximo, la puntuación de la propuesta se calculó aplicando la fórmula o procedimiento que se describe en el apartado 6, numeral 6.1.1 Matriz de Puntos, y numeral 17. Método de evaluación de propuestas del Anexo 2.- "Términos y Condiciones", ambos de la Convocatoria y los parámetros dispuestos en cada uno de ellos.----------

La puntuación de las proposiciones que cumplieron con los Requisitos de participación y documentación indispensable que los licitantes deberán de entregar para la Evaluación Técnica se describe a continuación: ----------

| No. | Licitante | Partida | Capacidad del licitante | Experiencia y Especialidad | Propuesta de Trabajo | Cumplimiento de Contratos | Total (TPT) |
|---|---|---|---|---|---|---|---|
| 1 | Totalsec, S.A. de C.V. en participación conjunta con Total Play Telecomunicaciones, SAPI de C.V. | 1 | 19.20 | 18.00 | 12.00 | 6.00 | **55.20** |
| 2 | Operbes, S.A. de C.V., en participación conjunta con Silent4Bussines, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V. | 1 | 23.10 | 18.00 | 12.00 | 6.00 | **59.10** |
| 3 | Axtel, S.A.B. de C.V. | 2 | 22.50 | 18.00 | 12.00 | 6.00 | **58.50** |
| 4 | Consulting All Service In Telecom And Medice S. de R.L. de C.V., en participación conjunta con Bohmer Strategists, S. de R.L. de C.V. y Secure Labs, S.A. de C.V. | 2 | 23.00 | 18.00 | 12.00 | 5.00 | **58.00** |
| 5 | Mnemo Evolution & Integration Services México, S.A. de C.V., en participación conjunta con Software Express S.A de C. V. | 2 | 21.90 | 9.00 | 12.00 | 3.00 | **45.90** |
| 6 | PG Ranhtoe Servicios Administrativos, S.A. de C.V. | 2 | 10.00 | 0.00 | 12.00 | 0.00 | **22.00** |
| 7 | Scitum S.A. de C.V. | 2 | 23.00 | 18.00 | 12.00 | 6.00 | **59.00** |
| 8 | Sixsigma Networks México, S.A. de C.V. en participación conjunta con SM4RT Security Services, S.A. de C.V. y B Drive It, S.A. de C.V. | 2 | 23.00 | 18.00 | 12.00 | 6.00 | **59.00** |

De la evaluación realizada, se desprende que el licitante **PG Ranhtoe Servicios Administrativos, S.A. de C.V. NO resulta solvente técnicamente**, en virtud de que, de acuerdo a la evaluación técnica



ANEXOS
DIVISIÓN DE CONTRATOS

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-E182-2022
OBJETO DE LA LICITACIÓN: SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024.

conforme a la Matriz de Puntos y los parámetros dispuestos en cada uno de ellos, no obtuvo una calificación igual o superior a 45 puntos de los 60 máximos que se pueden obtener. ----------

**D. EVALUACIÓN DE LAS PROPUESTAS ECONÓMICAS.** ----------

Solo las propuestas técnicas que resultaron solventes por haber obtenido una puntuación igual o superior a **45 puntos,** serán consideradas para realizar la evaluación de las proposiciones económicas. ----------

La evaluación de la propuesta económica de los licitantes: **1)** Totalsec, S.A. de C.V. en participación conjunta con Total Play Telecomunicaciones, SAPI de C.V., **2)** Operbes, S.A. de C.V., en participación conjunta con Silent4Bussines, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V., **3)** Axtel, S.A.B. de C.V., **4)** Consulting All Service In Telecom And Medice S. de R.L. de C.V., en participación conjunta con Bohmer Strategists, S. de R.L. de C.V. y Secure Labs, S.A. de C.V., **5)** Mnemo Evolution & Integration Services México, S.A. de C.V., en participación conjunta con Software Express S.A de C. V., **6)** Scitum S.A. de C.V. y **7)** Sixsigma Networks México, S.A. de C.V. en participación conjunta con SM4RT Security Services, S.A. de C.V. y B Drive it, S.A. de C.V.; quienes resultaron solventes técnicamente, fue realizada por parte de la División de Contratación de Activos y Logística de la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos, de conformidad con el numeral 7.1.3.1.2.3. del Manual de Organización de la Dirección de Administración y el numeral 5.3.8 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de este Instituto vigentes, conforme a lo siguiente: ----------

Para determinar la puntuación que corresponde a la propuesta económica de los licitantes, se utilizó la siguiente formula: ----------

PPE = MPemb x 40 / MP*i*. ----------

Donde: ----------

PPE = Puntuación que corresponde a la Propuesta Económica; ----------

MPemb = Precio Unitario ofertado más bajo, y ----------

MP*i* = Monto de la i-ésima Propuesta económica (Precio Unitario); ----------

**Partida 1.** Para efectos del cálculo de la puntuación que corresponde a la propuesta económica se utilizará la sumatoria de los precios unitarios (Sin IVA) de la Partida 1 del licitante, **Operbes, S.A. de C.V., en participación conjunta con Silent4Bussines, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V.** con **$92,657,867.00** (Noventa y dos millones, seiscientos cincuenta y siete mil, ochocientos sesenta y siete pesos 00/100, M.N.) sin considerar el IVA, que representa al Precio Unitario ofertado más bajo (MPemb). El cálculo se ilustra en la tabla siguiente: ----------

| No. | Licitante | Suma de precios unitarios MPi | PPE = MPemb x 40 / MPi | Asignación de Puntos PPE |
|---|---|---|---|---|
| 1.- | Operbes, S.A. de C.V., en participación conjunta con Silent4Bussines, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V. | $92,657,867.00 | 92,657,867 x 40 = 3,706,314,680<br><br>3,706,314,680 / 92,657,867 = 40 | **40.00** |

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-E182-2022
OBJETO DE LA LICITACIÓN: SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024.

| | | | | |
|---|---|---|---|---|
| 2.- | Totalsec, S.A. de C.V. en participación conjunta con Total Play Telecomunicaciones, SAPI de C.V. | $128,819,681.00 | 92,657,867 x 40 = 3,706,314,680<br><br>3,706,314,680 / 128,819,681 = 28.77 | **28.77** |

**Partida 2**. Para efectos del cálculo de la puntuación que corresponde a la propuesta económica se utilizará la sumatoria de los precios unitarios (Sin IVA) de la Partida 2 del licitante, **Mnemo Evolution & Integration Services México, S.A. de C.V., en participación conjunta con Software Express S.A de C. V.,** con **$149,412.54** (Ciento cuarenta y nueve mil, cuatrocientos doce pesos 54/100, M.N.) sin considerar el IVA, que representa al Precio Unitario ofertado más bajo (MPemb). El cálculo se ilustra en la tabla siguiente:

| No. | Licitante | Suma de precios unitarios MPi | PPE = MPemb x 40 / MPi | Asignación de Puntos PPE |
|---|---|---|---|---|
| 1.- | Axtel, S.A.B. de C.V. | $797,897.29 | 149,412.54 x 40 = 5,976,501.60<br><br>5,976,501.60 / 797,897.29 = 7.49 | **7.49** |
| 2.- | Consulting All Service In Telecom And Medice S. de R.L. de C.V., en participación conjunta con Bohmer Strategists, S. de R.L. de C.V. y Secure Labs, S.A. de C.V. | $204,017.85 | 149,412.54 x 40 = 5,976,501.60<br><br>5,976,501.60 / 204,017.85 = 29.29 | **29.29** |
| 3.- | Mnemo Evolution & Integration Services México, S.A. de C.V., en participación conjunta con Software Express S.A de C. V. | $149,412.54 | 149,412.54 x 40 = 5,976,501.60<br><br>5,976,501.60 / 149,412.54 = 40 | **40.00** |
| 4.- | Scitum S.A. de C.V. | $513,561.00 | 149,412.54 x 40 = 5,976,501.60<br><br>5,976,501.60 / 513,561 = 11.64 | **11.64** |
| 5.- | Sixsigma Networks México, S.A. de C.V. en participación conjunta con SM4RT Security Services, S.A. de C.V. y B Drive It, S.A. de C.V. | $298,190.90 | 149,412.54 x 40 = 5,976,501.60<br><br>5,976,501.60 / 298,190.90 = 20.04 | **20.04** |

ANEXOS
DIVISIÓN DE CONTRATOS

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-E182-2022
OBJETO DE LA LICITACIÓN: SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024.

**E. EVALUACIÓN FINAL.**

Para calcular el resultado final de la puntuación que obtuvo la proposición, se aplicó la siguiente fórmula:

**PTj = TPT + PPE** Para toda j = 1, 2,....,n

Dónde:

**PTj** = Puntuación Total de la proposición;

**TPT** = Total de Puntuación asignados a la propuesta Técnica;

**PPE** = Puntuación asignados a la Propuesta Económica.

El subíndice **"j"** representa a las demás proposiciones determinadas solventes como resultado de la evaluación.

La puntuación total obtenida por los licitantes se indica a continuación:

| Partida | No. | Licitante | Puntuación Técnica (TPT) | Puntuación Económica (PPE) | Puntuación Total (PTj) |
|---|---|---|---|---|---|
| 1 | 1.- | **Operbes, S.A. de C.V., en participación conjunta con Silent4Bussines, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V.** | **59.10** | **40.00** | **99.10** |
| | 2.- | Totalsec, S.A. de C.V. en participación conjunta con Total Play Telecomunicaciones, SAPI de C.V. | 55.20 | 28.77 | 83.97 |

| Partida | No. | Licitante | Puntuación Técnica (TPT) | Puntuación Económica (PPE) | Puntuación Total (PTj) |
|---|---|---|---|---|---|
| 2 | 1.- | Axtel, S.A.B. de C.V. | 58.50 | 7.49 | 65.99 |
| | **2.-** | **Consulting All Service In Telecom And Medice S. de R.L. de C.V., en participación conjunta con Bohmer Strategists, S. de R.L. de C.V. y Secure Labs, S.A. de C.V.** | **58.00** | **29.29** | **87.29** |
| | 3.- | Mnemo Evolution & Integration Services México, S.A. de C.V., en participación conjunta con Software Express S.A de C. V. | 45.90 | 40.00 | 85.90 |
| | 4.- | Scitum S.A. de C.V. | 59.00 | 11.64 | 70.64 |
| | 5.- | Sixsigma Networks México, S.A. de C.V. en participación conjunta con SM4RT Security Services, S.A. de C.V. y B Drive It, S.A. de C.V. | 59.00 | 20.04 | 79.04 |

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-E182-2022
OBJETO DE LA LICITACIÓN: SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024.

## III. RELACIÓN DE LICITANTES CUYAS PROPOSICIONES SE DESECHARON.

Se incluye un cuadro resumen de los licitantes cuyas propuestas se desecharon, con la expresión sintética del motivo ----------

| Partida. | Licitante | Motivo de Desechamiento |
|---|---|---|
| 2 | PG Ranhtoe Servicios Administrativos, S.A. de C.V. | No obtuvo calificación igual o superior a 45 puntos en la evaluación de su propuesta técnica. |

## IV. RELACIÓN DE LICITANTES CUYAS PROPOSICIONES RESULTARON SOLVENTES.

| Partida | Licitantes |
|---|---|
| 1 | Operbes, S.A. de C.V., en participación conjunta con Silent4Bussines, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V. |
| | Totalsec, S.A. de C.V. en participación conjunta con Total Play Telecomunicaciones, SAPI de C.V. |
| 2 | Axtel, S.A.B. de C.V. |
| | Consulting All Service In Telecom And Medice S. de R.L. de C.V., en participación conjunta con Bohmer Strategists, S. de R.L. de C.V. y Secure Labs, S.A. de C.V. |
| | Mnemo Evolution & Integration Services México, S.A. de C.V., en participación conjunta con Software Express S.A de C. V. |
| | Scitum S.A. de C.V. |
| | Sixsigma Networks México, S.A. de C.V. en participación conjunta con SM4RT Security Services, S.A. de C.V. y B Drive It, S.A. de C.V. |

## V. FALLO.

Con sustento en las evaluaciones que anteceden y que son el fundamento y soporte de esta decisión, con apego a lo establecido en los artículos 36, 36 Bis fracción I y 37 de la Ley; 52 del Reglamento; así como en el apartado 6. Criterios Específicos Conforme a los Cuales se Evaluarán las Proposiciones, la Maestra Elia Sandra Varas Galeana, Titular de la División de Contratación de Activos y Logística de la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos, de conformidad con los numerales 7.1.3.1.2.3 del Manual de Organización de la Dirección de Administración y el numeral 5.3.8 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de este Instituto vigentes, emite el Fallo del procedimiento de Licitación Pública Electrónica de Carácter Nacional con número de identificación en CompraNet **LA-050GYR019-E182-2022.** ----------

ANEXOS

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-E182-2022
OBJETO DE LA LICITACIÓN: SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024.

Con fundamento en los artículos 36, 36 Bis fracción I 37 y 46 de la LAASSP; 52 del Reglamento, así como el apartado 6. Criterios Específicos Conforme a los Cuales se Evaluarán las Proposiciones, por las razones expuestas, ya que cumplen con los requisitos legales, sus propuestas técnicas son solventes y al obtener en el resultado en la evaluación final una puntuación satisfactoria, se **ADJUDICAN** los **"Servicios Administrados de Seguridad Informática (SASI) 2022-2024"**, de la forma siguiente:----------

---

**Partida 1** al Licitante: **Operbes, S.A. de C.V., en participación conjunta con Silent4Bussines, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V.**----------

---

**Partida 2** al licitante: **Consulting All Service In Telecom And Medice S. de R.L. de C.V., en participación conjunta con Bohmer Strategists, S. de R.L. de C.V. y Secure Labs, S.A. de C.V.** --------

---

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. -----

---

De conformidad con lo señalado por el artículo 37 fracción V, de la LAASSP se informa a los licitantes ganadores que, a través de la persona que cuente con las facultades para este efecto, deberá presentarse a firmar el contrato dentro de los próximos 15 días naturales en la División de Contratos, de la Coordinación Técnica de Planeación y Contratos de este Instituto, en las oficinas ubicadas en la Calle de Durango No. 291, piso 10, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, Ciudad de México en horas hábiles con un horario de 9:30 a 14:00 y de 16:00 a 18:00 horas, para ello es necesario que a partir del día hábil siguiente al de la emisión de este Fallo, entregue la documentación requerida en el punto "3.11.- Fallo y firma de contrato" de la convocatoria a la licitación que nos ocupa. ----------

---

Asimismo, los licitantes adjudicados deberán entregar en la División de Contratos en el domicilio referido en el párrafo anterior, a más tardar dentro de los 10 días naturales siguientes a la firma del contrato, la garantía de cumplimiento del mismo. ----------

---

En cumplimiento a los artículos 2 fracción II, 45 último párrafo, 56 segundo párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP); 84 segundo párrafo de su Reglamento; así como lo establecido en el Acuerdo por el que se incorpora como un módulo de CompraNet la aplicación denominada Formalización de Instrumentos Jurídicos y se emiten las Disposiciones de carácter general que regulan su funcionamiento, publicado en el Diario Oficial de la Federación; se solicita que previo a la suscripción del contrato respectivo, el Representante Legal del Adjudicado lleve a cabo su registro en el Módulo de Formalización de Instrumentos Jurídicos (MFIJ), para lo cual se pone a su disposición las siguientes direcciones electrónicas: ----------

---

https://www.gob.mx/compranet/documentos/modulo-de-formalización-de-instrumentos-juridicos
https://compranetinfo.hacienda.gob.mx/descargas/Guia_de_registro_de_empresas_V3.pdf
https://procura-compranet.hacienda.gob.mx/proveedor/#/

---

En cumplimiento al artículo 84 del Reglamento de la LAASSP y las modificaciones establecidas en el DECRETO por el que se reforman y adicionan diversas disposiciones del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, publicado en el Diario Oficial de la Federación el 1° de junio de 2022, se señalan los datos de los contratos derivados del presente procedimiento conforme a lo siguiente: ----------

---



Ricardo Flores

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-E182-2022
OBJETO DE LA LICITACIÓN: SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024.

| **Partida 1 Datos del contrato y su garantía**<br>**Licitante adjudicado: Operbes, S.A. de C.V., en participación conjunta con Silent4Bussines, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V** | |
|---|---|
| Número de contrato: | 019E18222-001 |
| Objeto: | Servicios Administrados de Seguridad Informática (SASI) 2022-2024. Partida 1: 1. Servicios de Seguridad - Continuidad Operativa, 2. Servicios de Seguridad – Verificación y Calidad, 3. Servicios del Centro de Operaciones de Seguridad (SOC). |
| Monto: | Mínimo $138,499,360.00 (Ciento treinta y ocho millones, cuatrocientos noventa y nueve mil, trescientos sesenta pesos 00/100 M.N.), incluyendo el Impuesto al Valor Agregado. |
| | Máximo $346,248,400.00 (Trescientos cuarenta y seis millones, doscientos cuarenta y ocho mil, cuatrocientos pesos 00/100 M.N.), incluyendo el Impuesto al Valor Agregado. |
| Vigencia: | La vigencia del contrato será a partir del día hábil siguiente a la notificación del fallo y hasta el 30 de septiembre de 2024. |
| Porcentaje de la garantía | 10% (diez por ciento) del importe máximo del contrato antes del Impuesto al Valor Agregado (IVA). |
| Monto de la garantía | $29,849,000.00 (Veintinueve millones, ochocientos cuarenta y nueve mil pesos 00/100 M.N.) |
| Tipo de garantía: | Divisible. |

| **Partida 2 Datos del contrato y su garantía**<br>**Licitante adjudicado: Consulting All Service In Telecom And Medice S. de R.L. de C.V., en participación conjunta con Bohmer Strategists, S. de R.L. de C.V. y Secure Labs, S.A. de C.V.** | |
|---|---|
| Número de contrato: | 019E18222-002 |
| Objeto: | Servicios Administrados de Seguridad Informática (SASI) 2022-2024. Partida 2: 1. Análisis de Vulnerabilidades Estático, 2. Análisis de Vulnerabilidades Dinámico, 3. Servicios de Análisis Forense, 4. Servicios de Pruebas de Penetración. |
| Monto: | Mínimo $18,192,658.00 (Dieciocho millones, ciento noventa y dos mil, seiscientos cincuenta y ocho pesos 00/100 M.N.) incluyendo el Impuesto al Valor Agregado. |
| | Máximo $45,481,645.01 (Cuarenta y cinco millones, cuatrocientos ochenta y un mil, seiscientos cuarenta y cinco pesos 01/100 M.N.), incluyendo el Impuesto al Valor Agregado. |
| Vigencia: | La vigencia del contrato será a partir del día hábil siguiente a la notificación del fallo y hasta el 30 de septiembre de 2024. |
| Porcentaje de la garantía | 10% (diez por ciento) del importe máximo del contrato antes del Impuesto al Valor Agregado (IVA). |
| Monto de la garantía | $3,920,831.47 (Tres millones, novecientos veinte mil, ochocientos treinta y un pesos 47/100 pesos 00/100 M.N.) |
| Tipo de garantía: | Divisible. |

Los montos mínimos y máximos, incluyendo el IVA por ejercicio fiscal serán los siguientes:----------

ANEXOS
DIVISIÓN DE CONTRATOS

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-E182-2022
OBJETO DE LA LICITACIÓN: SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024.

| PARTIDA 1 | | | | |
|---|---|---|---|---|
| MONTOS | AÑO | | | TOTAL |
| | 2022 | 2023 | 2024 | |
| MÁXIMO | $43,281,050.00 | $173,124,200.00 | $129,843,150.00 | $346,248,400.00 |
| MÍNIMO | $17,312,420.00 | $69,249,680.00 | $51,937,260.00 | $138,499,360.00 |
| **PARTIDA 2** | | | | |
| MONTOS | AÑO | | | TOTAL |
| | 2022 | 2023 | 2024 | |
| MÁXIMO | $5,685,205.63 | $22,740,822.50 | $17,055,616.88 | $45,481,645.01 |
| MÍNIMO | $2,274,082.25 | $9,096,329.00 | $6,822,246.75 | $18,192,658.00 |

## VI. CIERRE DEL ACTA

Para efectos de la notificación y en términos del artículo 37 Bis de la LAASSP, a partir de esta fecha se pone a disposición de los licitantes, copia de esta acta en el mural de comunicación, situado en las oficinas de la División de Contratación de Activos y Logística, ubicada en: Calle Durango Núm. 291, quinto piso, Colonia Roma Norte, Código Postal 06700, Demarcación Territorial Cuauhtémoc, Ciudad de México, por un término no menor de cinco días hábiles, siendo de la exclusiva responsabilidad de los licitantes, acudir a enterarse de su contenido y obtener copia de la misma. Se difundirá un ejemplar de la presente acta en CompraNet https://compranet.hacienda.gob.mx/web/login.html. Dicho procedimiento sustituye a la notificación personal.

Asimismo, se les preguntó a los asistentes si deseaban manifestar alguna observación al mismo, a lo que, en el uso de la palabra, el representante del Órgano Interno de Control en el IMSS manifiesta lo siguiente:

Con fundamento en el artículo 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, que dispone que la Secretaría de la Función Pública, podrá verificar en cualquier tiempo, que las adquisiciones, arrendamientos y servicios se realicen conforme con lo establecido en la Ley de la materia y demás disposiciones aplicables, en correlación con el artículo 83, párrafo cuarto del Reglamento Interior del Instituto Mexicano del Seguro Social.

En este acto, una vez que se dio lectura a la presente acta, señalo que corresponde a las áreas requirente y técnica, en términos de los artículos 37 de la LAASSP y, 2 de su Reglamento, en correlación con el numeral 5.3.8, inciso a), de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social, verificar que los bienes o servicios que se evaluaron cumplen con la Convocatoria y sus anexos; con las precisiones de la Junta de aclaraciones y si las proposiciones que se presentaron cumplen con lo anterior, así como la debida asignación de los puntos y que se cuente con el debido sustento en los desechamientos, que en su caso, se hayan determinado.

Asimismo, se señala que es responsabilidad del área contratante y/o técnica, la evaluación que se realizó para la emisión del presente Acto de Fallo de conformidad con el artículo 36 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en concordancia con los numerales

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-E182-2022
OBJETO DE LA LICITACIÓN: SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024.

4.2.2.1.15, 4.2.2.1.16 y 4.2.2.1.17 del Acuerdo por el que se expide el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público. ----------

No habiendo otro hecho que hacer constar, se da por terminado este acto, siendo las **11:55 horas día en que se actúa,** firmando quien preside, para los efectos legales, administrativos y de notificación a que haya lugar. ----------

Este Fallo consta de **13 (trece)** páginas, anexándose **3 (tres)** páginas de las propuestas económicas de los licitantes adjudicados y dos anexos constantes de **200 (doscientas)** páginas, firmando para los efectos legales y de conformidad, por quien emite el Fallo y la asiste. ----------

**FIN DE TEXTO**

**Por el Instituto Mexicano del Seguro Social:** ----------

| | |
|---|---|
| Titular de la División de Contratación de Activos y Logística<br>(Área Contratante) | **Mtra. Elia Sandra Varas Galeana** |
| Titular de la División de Seguridad Informática Física<br>(Área Requirente y Técnica) | **Ing. Abraham Gutiérrez Castillo** |
| Representante de la Coordinación de Legislación y Consulta | **Lic. Mayra Selene García Aguilar** |
| Representante del Órgano Interno de Control en el IMSS | **Lic. Sergio Emilio Segura Ortega** |

Las firmas que anteceden corresponden al Acta de Fallo del procedimiento de Licitación Pública Nacional Electrónica número **LA-050GYR019-E182-2022.** ----------

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

# ATENTA NOTA

Ciudad de México, a 18 de octubre de 2022.

**Para: Lic. Humberto Rincón Juárez**
Titular de la División de Contratos.

**De: Mtra. Elia Sandra Varas Galeana**
Titular de la División de Contratación de Activos y Logística.

Me refiero a la documentación remitida con mi oficio número 09 53 84 61 1CFJ/2022/10317, para la elaboración de los instrumentos jurídicos número 019E18222-001 y 019E18222-002, derivados del procedimiento de Licitación Pública Nacional Electrónica, número LA-050GYR019-E182-2022, para la contratación de los "Servicios Administrados de Seguridad Informática (SASI) 2022-2024"

Al respecto del Acta de Fallo, me permito aclararlo siguiente:

**Dice:**
Operbes, S.A. de C.V., en participación conjunta con **Silent4Bussines**, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V.

**Debe Decir:**
Operbes, S.A. de C.V., en participación conjunta con **Silent4Business**, S.A. de C.V. y Bufete Empresarial GTI, S.A. de C.V.

Sin más por el momento, aprovecho la ocasión de enviarle un cordial saludo.

Atentamente

INSTITUTO MEXICANO DEL SEGURO SOCIAL
COORDINACIÓN TÉCNICA DE
18 OCT 2022
RECIBIDO
DIVISIÓN DE CONTRATOS

**ANEXOS**
**DIVISIÓN DE CONTRATOS**

SIN TEXTO

| | | |
|---|---|---|
| IMSS | INSTITUTO MEXICANO DEL SEGURO SOCIAL<br>DIRECCIÓN DE ADMINISTRACIÓN<br>UNIDAD DE ADQUISICIONES<br>COORDINACIÓN DE ADQUISICIÓN DE BIENES Y<br>CONTRATACIÓN DE SERVICIOS<br>COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS | CONTRATO<br>NÚMERO<br>019E18222-001 |

# ANEXO 4 (CUATRO)

## "DOCUMENTO DE DESIGNACIÓN DE ADMINISTRADOR DEL CONTRATO"

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

GOBIERNO DE MÉXICO | IMSS

DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TÉCNOLOGICO
Coordinación de Telecomunicaciones y Seguridad de la Información

Of Nº 09 52 17 61 5A00/2022/0185

Ciudad de México, a 09 de agosto de 2022

**Ing. Abraham Gutiérrez Castillo**
Titular de la División de Seguridad
Informática Física
P r e s e n t e

Me refiero al procedimiento de contratación de los "**Servicios Administrados de Seguridad Informática (SASI) 2022-2024"**, con fecha de inicio al día hábil siguiente de la notificación de fallo y hasta el 30 de septiembre de 2024.

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, le informo que esa División a su cargo, ha sido designada para fungir como área técnica y administradora 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 y numerales 2, 4.17, 4.25 y 5.3.15 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social.

Asimismo, los exhorto a desempeñar el cargo que le ha sido conferido y que se formalizará mediante la suscripción del instrumento jurídico que derive del procedimiento de contratación en comento, con la mayor diligencia, en estricto apego en las leyes de la materia y a los principios de legalidad, honradez, lealtad, imparcialidad y eficiencia que rigen el servicio público federal.

Sin otro particular por el momento, hago propicia la ocasión para enviarles un cordial saludo.

**Atentamente**

**Lic. Florencio Fernando González Velázquez**
Titular de la Coordinación de Telecomunicaciones y
Seguridad de la Información

FGV/COVV/jom

IMSS DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO
09 AGO 2022
División de Seguridad Informática Física



ANEXOS
DIVISIÓN DE CONTRATOS

2022 Ricardo Flores Magón
Año de

SIN TEXTO

| | | |
|---|---|---|
| IMSS | INSTITUTO MEXICANO DEL SEGURO SOCIAL<br>DIRECCIÓN DE ADMINISTRACIÓN<br>UNIDAD DE ADQUISICIONES<br>COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS<br>COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS | CONTRATO NÚMERO 019E18222-001 |

# ANEXO 5 (CINCO)

## "JUNTA DE ACLARACIONES, LA CUAL SE ENCUENTRA DISPONIBLE PARA SU CONSULTA EN COMPRANET"

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

# "JUNTA DE ACLARACIONES DISPONIBLE PARA SU CONSULTA EN EL PORTAL DE COMPRAS GUBERNAMENTALES COMPRANET"

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

# ANEXO 6 (SEIS)

# "CONVENIO DE PARTICIPACIÓN CONJUNTA"

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

# DOCUMENTACIÓN LEGAL

# 1.3.8 ANEXO 15
# CONVENIO PROPOSICIÓN CONJUNTA

ANEXOS
DIVISIÓN DE CONTRATOS

## MANIFIESTO DE PARTICIPACIÓN EN CONJUNTA

Ciudad de México, a 30 de septiembre de 2022.

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

**Procedimiento Número:** LA-050GYR019-E182-2022

Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes, en nuestro carácter de apoderados legales de la empresa Operbes, S.A. de C.V., actuando como representante común de la participación conjunta de las empresas Silent4Business, S.A. de C.V., Bufete Empresarial GTI, S.A. de C.V., y Operbes, S.A. de C.V., manifestamos que es interés y voluntad de nuestra representada participar de manera conjunta con las empresas antes mencionadas para la partida 1 del presente proceso de Licitación.

Protestamos lo necesario

Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes
Apoderados Legales de Operbes, S.A. de C.V., actuando como Representante Común de la Participación Conjunta de las empresas Bufete Empresarial GTI, S.A. de C.V., Silent4Busines, S.A. de C.V., y Operbes, S.A. de C.V.

## MANIFIESTO DE PARTICIPACIÓN EN PARTIDA 1

Ciudad de México, a 30 de septiembre de 2022.

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

**Procedimiento Número:** LA-050GYR019-E182-2022

Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes, en nuestro carácter de apoderados legales de la empresa Operbes, S.A. de C.V., actuando como representante común de la participación conjunta de las empresas Silent4Business, S.A. de C.V., Bufete Empresarial GTI, S.A. de C.V., y Operbes, S.A. de C.V., manifestamos que es interés y voluntad de nuestra representada participar en la **partida 1** del presente proceso de Licitación.

Protestamos lo necesario

Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes
Apoderados Legales de Operbes, S.A. de C.V., actuando como Representante Común de la Participación Conjunta de las empresas Bufete Empresarial GTI, S.A. de C.V., Silent4Busines, S.A. de C.V., y Operbes, S.A. de C.V.



ANEXOS
DIVISIÓN DE CONTRATOS

Convenio de Participación Conjunta (" **El Convenio**") que celebran por una parte, el participante **Operbes, S.A. de C.V.** representada en este acto **por Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes**, en su carácter de apoderados legales, a quien en lo sucesivo se le denominará "**El Participante A**"; por otra parte el participante **Silent4Business, S.A. de C.V.**, representada en este acto por **Gerardo Garibay Aymes** en su carácter de representante legal legales, a quien en lo sucesivo se le denominará "**El Participante B**", por otra parte el participante **Bufete Empresarial GTI, S.A. de C.V.**, representada en este acto por **Juan Luis Pineda González** en su carácter de representante legal legales, a quien en lo sucesivo se le denominará "**El Participante C**", las personas morales antes señaladas aceptan de manera libre y voluntaria sujetarse al fiel y exacto cumplimiento de las obligaciones que se establecen en el presente convenio; las personas morales antes referidas se denominarán en forma conjunta como las "partes". El presente convenio se formaliza con motivo del procedimiento de **Licitación Pública Nacional Electrónica** Núm. **LA-050GYR019-E182-2022** en lo sucesivo la "Licitación", para la contratación de los **"Servicios Administrados de Seguridad Informática (SASI) 2022-2024",** convocada por el **Instituto Mexicano del Seguro Social** en lo sucesivo "La Convocante", y cuando se haga referencia a los que intervienen se denominarán "Las Partes" al tenor de las siguientes declaraciones y cláusulas:

## DECLARACIONES

### 1. El Participante A, declara a través de sus apoderados legales, que:

**1.1** Ser una sociedad legalmente constituida de conformidad con las leyes mexicanas, bajo la denominación "Operadora Bestel, S.A. de C.V." según consta en el testimonio de la escritura pública 16,515, de fecha 22 de marzo de 2007, otorgada ante la fe del Lic. Felipe Ignacio Vázquez Aldana Sauza, Notario Público 9 de la municipalidad de Tlaquepaque, Jalisco, en la cual se hizo constar la constitución de la sociedad denominada Operadora Bestel, S. A. de C.V., cuyo primer testimonio quedó inscrito en el folio mercantil 37737*1, el 13 de agosto de 2007 en el Registro Público de la Propiedad y del Comercio de Guadalajara, Jalisco.

**1.2.** Las reformas que ha sufrido:
**1.- Escritura Pública número 16,970** de fecha 3 de Julio de 2007, otorgada ante la fe del Lic. Felipe Ignacio Vázquez Aldana Sauza, Notario Público No. 9 de la Municipalidad de Tlaquepaque, Jalisco, se hizo constar: uno. - el cambio de denominación social de Operadora Bestel, S.A. de C.V. a Operbes, S.A. de C.V.; dos: La modificación en consecuencia de la cláusula primera de los estatutos sociales. Quedando registrada en el Registro Público de la Propiedad y del Comercio de Guadalajara Jalisco, bajo el folio mercantil electrónico 37737*1 de fecha 17 de octubre de 2007.

**2.- Escritura Pública número 17,121** de fecha 26 de julio de 2007, otorgada ante la fe del Lic. - Felipe Ignacio Vázquez Aldana Sauza, Notario Público No. 9 de la Municipalidad de Tlaquepaque, Jalisco, se hizo constar: uno. - la adición de un segundo párrafo a la cláusula sexta de los estatutos de la sociedad; dos-.la reforma a la cláusula Décima Primera de los estatutos de la sociedad. Quedando registrada en el Registro Público de la Propiedad y del



000

Comercio de Guadalajara Jalisco, bajo el folio mercantil electrónico 37737*1, con fecha 01 de julio de 2008.

**3.- Escritura Pública número 17,540** de fecha 11 de octubre de 2007, otorgada ante la fe del Lic. Felipe Ignacio Vázquez Aldana Sauza, Notario Público No. 9 de la Municipalidad de Tlaquepaque, Jalisco, se hizo constar: uno: La modificación a la cláusula Décima Primera de los estatutos sociales; dos: La modificación de la cláusula Décima Primera de manera automática al momento en que la sociedad adquiriera el carácter de concesionario para la instalación, operación y explotación de redes públicas de telecomunicaciones interestatales, en términos de la legislación aplicable. Quedando registrada en el Registro Público de la Propiedad y del Comercio de Guadalajara Jalisco, bajo el folio mercantil electrónico 37737, con fecha 15 de mayo de 2019.

**4.- Escritura Pública número 63,351** de fecha 14 de octubre de 2008, otorgada ante la fe del Lic. Rafael Manuel Oliveros Lara, notario Público No. 45 de la Ciudad de México, se hizo constar: uno: - Reforma a la cláusula décima Segunda de los estatutos sociales. Quedando registrada en el Registro Público de la Propiedad y del Comercio de Guadalajara Jalisco, bajo el folio mercantil electrónico 37737*1, con fecha 11 de noviembre de 2008.

**5.- Escritura Pública número 17,719** de fecha 15 de noviembre de 2007, otorgada ante la fe del Lic. Felipe Ignacio Vázquez Aldana Sauza, Notario Público No. 9 de la Municipalidad de Tlaquepaque, Jalisco, se hizo constar: uno: El aumento de capital en la parte variable del capital social e incorporación de Letseb. S.A. de C.V. como accionista. Quedando registrada en el Registro Público de la Propiedad y del Comercio de Guadalajara Jalisco, bajo el folio mercantil electrónico 37737*1, con fecha 27 de mayo de 2008.

**6.- Escritura Publica número 17,721** de fecha 15 de noviembre de 2007, otorgada ante la fe del Lic. Felipe Ignacio Vázquez Aldana Sauza, Notario Público No. 9 de la Municipalidad de Tlaquepaque, Jalisco, se hizo constar: uno: La adición de un segundo párrafo de la cláusula sexta, que implica un aumento de capital en la parte variable del capital social. Quedando registrada en el Registro Público de la Propiedad y del Comercio de Guadalajara Jalisco, bajo el folio mercantil electrónico 37737*1, con fecha 18 de junio de 2008.

**7.- Escritura Pública número 17,722** de fecha 15 de noviembre de 2007, otorgada ante la fe del Lic. Felipe Ignacio Vázquez Aldana Sauza, Notario Público No. 9 de la Municipalidad de Tlaquepaque, Jalisco, se hizo constar: a) se autorizó a el accionista Bestel, S.A. de C.V. (i) transmita, en favor de Letseb, S.A. de C.V., de la totalidad de las acciones Serie "A" y Serie "B" (incluyendo las acciones pagadoras) de las cuales es titular en la parte fija y en la parte variable del capital social de la sociedad (las "Acciones Bestel"), (ii)endose en propiedad los títulos de acciones que amparan la Acciones Bestel en favor de Letseb, S.A. de C.V.- b) Se autoriza e instruye al Administrador Único de la sociedad a efecto de reflejar dicha transmisión.- c) Se autoriza al Administrador Único de la Sociedad para que, una vez que se obtenga la autorización de la SCT y Bestel, S.A. de C.V. facture la transmisión de las concesiones a la sociedad, proceda con (i) la cancelación del título de acciones emitido en esta fecha respecto de las Acciones Pagadoras, y con la consecuente emisión, en favor de Bestel, S.a. de C.V. o Letseb, S.A- de C.V., según sea el caso, de un nuevo título de acciones que refleje que dichas Acciones Pagadoras se encuentran íntegramente suscritas, pagadas y liberadas; y (ii) entregue nuevo título de acciones a Bestel, S.A. de C.V. o Letseb, S.A. de C.V., según sea el caso. Quedando registrada en el Registro Público de la Propiedad y del Comercio de Guadalajara Jalisco, bajo el folio mercantil electrónico 37737*1 con fecha 18 de junio de 2008.

ANEXOS
DIVISIÓN DE CONTRATOS



000

SE CANCELAN DATOS PERSONALES DE PERSONA(S) MORALES IDENTIFICABLE(S) TALES COMO: NOMBRE Y RFC DE ACCIONISTAS DE EMPRESAS, POR CONSIDERARSE INHERENTE AL PATRIMONIO DE LA PERSONA MORAL, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN III Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016



**8.-Escritura Pública número 28,934** de fecha 19 de agosto de 2021, otorgada ante la fe del Lic. Manuel Enrique Oliveros Lara, Notario Público No. 100 de la Ciudad de México, se hizo constar entre otros acuerdos: uno. – Se reforman en su totalidad los estatutos sociales de la sociedad. Misma que se encuentra en trámite de inscripción en el Registro Público de la Propiedad y de Comercio de Guadalajara, Estado de Jalisco.

**1.3** Conforme a sus estatutos sociales vigentes, los accionistas que la integran son las siguientes personas:

- [redacted] (RFC: [redacted]
- [redacted] (RFC [redacted])

**1.4** La sociedad tiene como objeto social:

a. La prestación de todo tipo de servicios públicos de telecomunicaciones al amparo de las concesiones y/o autorizaciones de las que sea titular, otorgadas por la autoridad competente en México.
b. Usar, aprovechar y/o explotar bandas de frecuencias del espectro radioeléctrico en el territorio nacional para la prestación de servicios públicos de telecomunicaciones, al amparo de las concesiones y/o autorizaciones de las que sea titular, otorgadas por la autoridad competente en el país y/o mediante cualquier forma prevista por la normatividad vigente en México.
c. Ocupar posiciones orbitales geoestacionarias y órbitas satelitales asignadas al país, y explotar sus respectivas bandas de frecuencias.
d. Explotar los derechos de emisión y recepción de señales y bandas de frecuencias asociadas a sistemas satelitales extranjeros o nacionales que cubran y puedan prestar servicios en territorio nacional.
e. Adquirir, arrendar o disponer toda clase de infraestructura y equipos, y en general toda clase de bienes muebles e inmuebles necesarios o convenientes para la realización de los objetos de la Sociedad.
f. La integración a favor de terceros de bienes y servicios de carácter técnico, tecnológico, administrativo, de supervisión, de organización, de ingeniería y en general, cualquier clase de bienes o servicios relacionados con las telecomunicaciones y las tecnologías de la información y la comunicación, ya sean de proveedores nacionales o extranjeros, incluyendo obras.
g. Representar en calidad de agente, intermediario o mediador, comisionista, factor, consignatario, representante legal o mandatario de toda clase de empresas o personas nacionales o extranjeras, para la adquisición y/o comercialización y/o distribución de servicios públicos de telecomunicaciones
h. Obtener o conceder toda clase de préstamos o créditos con o sin garantía específica; realizar operaciones con toda clase de derivados; emitir, girar, aceptar, endosar o avalar pagarés, cheques, letras de cambio, obligaciones y toda clase de títulos de crédito; así como otorgar y obtener fianzas y garantías de cualquier clase respecto de obligaciones a cargo de la Sociedad o de terceros, actuando además como obligado solidario;
i. Adquirir, suscribir, comprar, permutar, disponer, enajenar, transmitir, ceder, gravar o, en general, negociar con todo tipo de acciones, partes sociales o participaciones en otras sociedades civiles o mercantiles, o adquirir acciones,

000

partes sociales o participaciones en cualesquier entidades previamente constituidas, así como disponer, enajenar, transmitir, ceder, gravar o, en general, negociar en cualquier forma tales acciones, partes sociales o participaciones;

j. Representar en calidad de agente, intermediario o mediador, comisionista, factor, consignatario, representante legal o mandatario de toda clase de empresas o personas nacionales o extranjeras;

k. Poseer por cualquier título legal toda clase de bienes muebles e inmuebles necesarios o convenientes para la realización de los objetos de la Sociedad;

l. Poseer por cualquier título legal toda clase de licencias de patentes, certificados de invención, marcas, nombres comerciales, secretos industriales, derechos de autor, así como licencias y concesiones de todo tipo, ya sea en México o en el extranjero;

m. Celebrar, suscribir, transmitir, ceder u operar todos los actos, contratos y convenios, incluyendo sin limitar cualesquier contratos de fideicomiso, que sean necesarios o convenientes para la realización del objeto de la Sociedad, en México o en el extranjero;

n. En general, realizar todos los actos y operaciones conexos, accesorios o accidentales, que sean necesarios o convenientes para la realización de los objetos anteriores.

**1.5** En este acto se encuentra representada por Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes, en su calidad de apoderados legales, quienes tienen domicilio en [redacted] y cuentan con todas las facultades necesarias para la celebración del presente **Convenio**, mismas que a la fecha no les han sido revocadas ni modificadas, circunstancia que acreditan con el testimonio de la Escritura Pública No. 25,706 de fecha 26 de febrero de 2018, pasada ante la fe del Notario Público Licenciado Manuel Enrique Oliveros Lara Notario Público Número 100 de la Ciudad de México, misma que se encuentra debidamente inscrita en el Registro Público de Comercio de Guadalajara, Jalisco, bajo el folio mercantil electrónico 37737, de fecha 19 de agosto de 2019.

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: DOMICILIO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN I Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016

**1.6** Se encuentra debidamente inscrito en el Registro Federal de Contribuyentes ante la Secretaría de Hacienda y Crédito Público, con el número OPE070326DNA y Registro Patronal ante el Instituto Mexicano del Seguro Social [redacted] y tiene su domicilio fiscal el ubicado en Avenida Javier Barros Sierra, número 540, Torre II, Colonia Lomas de Santa Fe, Alcaldía de Álvaro Obregón, C.P. 01219, Ciudad de México, mismo que señala para los fines y efectos legales de este **Convenio.**

**2 El Participante B, declara a través de sus apoderados legales, que:**

**2.1** Es una sociedad legalmente constituida conforme a las leyes de México, según consta en la escritura pública número No. 61,579, otorgada ante la fe del Notario Público número 246, en el protocolo de la notaría número 212, la cual se encuentra debidamente inscrita en el Registro Público de Comercio en la Ciudad de México, con el número de folio 561326-1 de fecha 08 de agosto 2016.

ANEXOS
DIVISIÓN DE CONTRATOS

SE CANCELAN DATOS PERSONALES DE PERSONA(S) MORALES IDENTIFICABLE(S) TALES COMO: REGISTRO PATRONAL, POR CONSIDERARSE INHERENTE AL PATRIMONIO DE LA PERSONA MORAL, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN III Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016



000

**2.2** Las reformas que ha sufrido:
Instrumento Número: 80,645
Fecha del instrumento: 19 de diciembre de 2017.
Nombre del Notario: Licenciado Moisés Farca Charabati.
Número del Notario: 91.
Lugar del Notario: Ciudad de México
Se protocolizó el acta de asamblea donde se modificó la tenencia accionaria y como consecuencia la exclusión y admisión de nuevos accionistas para quedar como actualmente se encuentra suscrito el capital social en su parte fija (accionistas Layla Esperanza Delgadillo Aguilar y Eduarda Delgadillo Aguilar).

Instrumento Número: 35,143
Fecha de la Escritura: 10 de septiembre de 2019.
Nombre del Notario: Licenciado Antonio Rosado Sánchez.
Número del Notario: 199
Lugar del Notario: Ciudad de México.
Se protocolizó el acta de asamblea donde se aumentó el capital social de Silent4business, S.A. de C.V. en [redacted] a su actual capital social variable, en total sumados el capital fijo y variable [redacted] así como la admisión de [redacted] como nuevo accionista debido a su aportación a la parte variable del capital social.

Instrumento Número: 65,123
Fecha del Instrumento: 08 de julio de 2020.
Nombre del Notario: Licenciado Héctor Manuel Cárdenas Villarreal.
Número del Notario: 201
Lugar del Notario: Ciudad de México
Modificación de la cláusula quinta de los estatus sociales, aumentar el capital social en su parte fija variable, así como reformar la cláusula quinta de los estatutos sociales.

Instrumento número: 65,124
Fecha del instrumento: 08 de julio del 2020
Nombre del Notario: Hector Manuel Cárdenas Villarreal
Número de Notario: 201
Lugar del Notario: Ciudad de México
Transmisión de acciones al capital variable.

Instrumento Número: 997
Fecha del Instrumento: 08 de marzo de 2021.
Nombre del Notario: Licenciado Gustavo Fernández Sauri.
Número del Notario: 184
Lugar del Notario: Estado de México
Acta Poder

**SE CANCELAN DATOS PERSONALES DE PERSONA(S) MORALES IDENTIFICABLE(S) TALES COMO: CAPITAL SOCIAL, NOMBRE DE SOCIOS O ACCIONISTAS DE EMPRESAS, POR CONSIDERARSE INHERENTE AL PATRIMONIO DE LA PERSONA MORAL, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN III Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016**

**SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE DE SOCIOS O ACCIONISTAS, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN I Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016**

**2.3** Conforme a sus estatutos sociales vigentes, los socios o accionistas que la integran son las siguientes personas:

[redacted]
Representada por: [redacted]

[redacted]
Representada por: [redacted]

SE CANCELAN DATOS PERSONALES DE PERSONA(S) MORALES IDENTIFICABLE(S) TALES COMO: NOMBRE DE SOCIOS O ACCIONISTAS DE EMPRESAS, POR CONSIDERARSE INHERENTE AL PATRIMONIO DE LA PERSONA MORAL, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN III Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE DE SOCIOS O ACCIONISTAS, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN I Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016



[redacted]

Representada por: [redacted]

**2.4** La sociedad tiene como objeto social:

La comercialización de servicios de información en el área de investigación técnica y científica, practicar toda clase de investigaciones y estudios sobre la potencialidad y tendencias de mercado, rendir toda clase de asesoría y servicios técnicos y especializados en el análisis, elaboración, mantenimiento, actualización y procedimiento electrónico de datos y estadísticas medicas o científicas y prestar servicios de consultoría en promoción de ventas, organización de seminarios y cursos en mercadotecnia para toda clase de sociedades o empresas de sector público o privado. Por lo que enunciativa y no limitativamente la sociedad podrá dedicarse a:

**A.** La compraventa, importación, exportación, comercialización, intermediación, y comisión de todo tipo de equipo de informática incluyendo el "software" y "hardware", así como todo tipo de paquetes relacionados con la informática.
**B.** Prestar servicios ya sean estos técnicos o de asesoría relacionados con la informática;
**C.** La adquisición, enajenación, distribución, comisión, importación, exportación, representación, consignación, promoción y comercialización en general por cuenta propia o ajena de toda clase de equipo de cómputo, tecnología, accesorios y sus derivados, así como toda clase de artículos y productos que se encuentren en el comercio y permitidos por la Ley;
**D.** Contratar activa o pasivamente toda clase de prestaciones de servicios, celebrar contratos, convenios, así como adquirir por cualquier título, patentes, marcas industriales, nombres comerciales, opciones y preferencias derechos de propiedad literaria, industrial, artística o concesiones de alguna autoridad;
**E.** La explotación de patentes, marcas, registros y nombres comerciales, sean propios o su explotación sea autorizada por terceras personas en relación con las actividades del objeto social.
**F.** Proporcionar servicios de consultoría en aspectos de informática, comerciales, gerenciales, administrativos y financieros;
**G.** Servicios y asesoría de análisis, desarrollo en sistemas y programación de computadoras;
**H.** La reparación de equipos de computación en general;
**I.** La configuración, ensamblado, distribución, almacenamiento, fabricación, instalación, reparación, soporte técnico, recolección, compra, venta, importación, exportación, mercadeo, representación, comisión, explotación, promoción, consignación, maquila, intermediación, difusión, mantenimiento, operación y el comercio en general con todo tipo de equipos de cómputo, eléctrico, electrónico, de comunicaciones, telecomunicaciones, computadoras, terminales, telefax, redes, "software", "hardware", "Internet•, "Intranet", insumos, consumibles, aparatos y dispositivos eléctricos. electrónicos, mecánicos, electromecánicos, trabajos de tecnologías de información y demás artículos y actividades relacionados con lo anterior;
**J.** La elaboración, diseño, implementación y desarrollo de todo tipo de sistemas, páginas "web", "Intranet", "extranet" e "Internet", portales de cualquier tipo y especie, fibra óptica, redes inalámbricas y cualquier otra actividad relacionada o conexa con lo anterior;

**K.** Formar parte, en cualquier forma legal de otras sociedades;
**L.** La capacitación y adiestramiento a personas físicas o morales, relacionadas con el

ANEXOS
DIVISIÓN DE CONTRATOS

objeto social;

**M.** Contratar al personal que la sociedad considere necesario para llevar a cabo su objeto social y delegar en una o varias personas el cumplimiento de mandatos, comisiones, servicios y demás actividades propias de su objeto, así como contratar los servicios de dirección técnica para capacitar al personal de la sociedad.

**N.** El establecimiento de toda clase de oficinas, agencias o sucursales, dentro y fuera de la República Mexicana, necesarios y convenientes para el desarrollo de su objeto social;

Ñ. Representar y ser agente comisionista o mediador en cualquier clase en operación realizada por la sociedad, ya sean personas físicas o morales, nacionales o extranjeras;

**O.** Formar parte de otras sociedades o empresas, adquiriendo acciones o partes sociales; participar en la administración o liquidación de toda clase de sociedades o empresas y emitir obligaciones;

**P.** La adquisición, enajenación, importación, exportación, arrendamiento o distribución por cuenta propia o ajena de toda clase de bienes muebles e inmuebles, materias primas, maquinaria, equipo, implementos, partes, refacciones o vehículos convenientes o necesarios para el desarrollo de los fines sociales anteriores;

**Q.** La adquisición, instalación, operación o alquiler por cuenta propia o ajena de toda clase de instalaciones, locales, expendios bodegas, almacenes u oficinas que en cualquier forma se relacionen con los objetos sociales anteriores; y en general la ejecución de toda clase de instalaciones, locales, expendios, bodegas, almacenes u oficinas que en cualquier forma se relacionen con los objetos sociales anteriores; y en general la ejecución de toda clase de actos y la celebración de toda clase de contratos que en cualquier forma tengan relación con los fines sociales antes indicados;

**R.** Otorgar, suscribir, aceptar, endosar o avalar toda clase de títulos de crédito conforme a lo dispuesto por la Ley General de Títulos y Operaciones de Crédito;

**S.** La realización de toda clase de actos materiales y jurídicos, por cuenta propia o ajena, incluyendo actos de dominio, y la celebración de los contratos o convenios civiles o mercantiles, principales o de garantía, o de cualquier otra especie, relacionados con los propósitos antes mencionados, y la realización de las operaciones industriales o mercantiles similares o conexas con las finalidades con las que se han aludido; y

**T.** En general la celebración y cumplimiento de toda clase de actos, operaciones y convenios necesarios, derivados o convenientes para la realización del objeto social, realizado ya sea por cuenta propia o de terceros.

2.5 En este acto se encuentra representada por Gerardo Garibay Aymes, en su calidad de representante legal, quienes tienen domicilio en [redacted] y cuentan con todas las facultades necesarias para la celebración del presente Convenio, mismas que a la fecha no les han sido revocadas ni modificadas, circunstancia que acredita con el testimonio del Instrumento No. 997 de fecha 08 de marzo de 2021, pasada ante la fe del Notario Público Lic. Gustavo Fernández Sauri Notario Público Número 184.

2.6 Se encuentra debidamente inscrito en el Registro Federal de Contribuyentes ante la Secretaría de Hacienda y Crédito Público, con el número SIL160727HV7 y Registro Patronal ante el Instituto Mexicano del Seguro [redacted] y tiene su domicilio fiscal Avenida Insurgentes Sur No. 2453, Piso 4, Colonia Tizapán San Ángel, Alcaldía Álvaro obregón, C.P. 01090, Ciudad de México, mismo que señala para los fines y efectos legales de este Convenio.

001

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: DOMICILIO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN I Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016



SE CANCELAN DATOS PERSONALES DE PERSONA(S) MORALES IDENTIFICABLE(S) TALES COMO: REGISTRO PATRONAL, POR CONSIDERARSE INHERENTE AL PATRIMONIO DE LA PERSONA MORAL, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN III Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016

3 El Participante C, declara a través de sus apoderados legales, que:

**3.1** Es una sociedad legalmente constituida conforme a las leyes de México, según consta en la escritura pública número No. 53,929, otorgada ante la fe del Notario Público número 226, la cual se encuentra debidamente inscrita en el Registro Público de Comercio en la Ciudad de México, con el número de folio 527176-1 de fecha 12 de diciembre 2014.

**3.2** Las reformas que ha sufrido:
Instrumento Número: 33,661
Fecha del instrumento: 26 de julio de 2019.
Nombre del Notario: Licenciada Rosamaría López Lugo.
Número del Notario: 223.
Lugar del Notario: Ciudad de México

Instrumento Número: 40,679
Fecha de la Escritura: 04 de febrero de 2021.
Nombre del Notario: Licenciado Alfredo Caso Velázquez.
Número del Notario: 17
Lugar del Notario: Estado de México.

Instrumento Número: 41,614
Fecha del Instrumento: 27 de agosto 2021.
Nombre del Notario: Licenciado Alfredo Caso Velázquez.
Número del Notario: 17
Lugar del Notario: Estado de México

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE DE SOCIOS O ACCIONISTAS Y DOMICILIO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN I Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016

**3.3** Conforme a sus estatutos sociales vigentes, los socios o accionistas que la integran son las siguientes personas:
[redacted]

**3.4** La sociedad tiene como objeto social:
La comercialización, producción, fabricación, importación y exportación, de toda clase de productos, así como la prestación de toda clase de servicios, a cualquier persona física o moral de naturaleza privada o pública.

**3.5** En este acto se encuentra representada por Juan Luis Pineda González, en su calidad de representante legal, quien tiene domicilio en [redacted] y cuentan con todas las facultades necesarias para la celebración del presente Convenio, mismas que a la fecha no les han sido revocadas ni modificadas, circunstancia que acredita con el testimonio del Instrumento No. 71,945 de fecha 11 de junio de 2019, pasada ante la fe del Notario Público Lic. Miguel Ángel Beltrán Lara Notario Público Número 169.

3.6 Se encuentra debidamente inscrito en el Registro Federal de Contribuyentes ante la Secretaría de Hacienda y Crédito Público, con el número BEG141128JD5 y Registro Patronal ante el Instituto Mexicano del Seguro [redacted] y tiene su domicilio

001

SE CANCELAN DATOS PERSONALES DE PERSONA(S) MORALES IDENTIFICABLE(S) TALES COMO: REGISTRO PATRONAL, POR CONSIDERARSE INHERENTE AL PATRIMONIO DE LA PERSONA MORAL, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 113 FRACCIÓN III Y 118 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 09-mayo-2016



ANEXOS
DIVISIÓN DE CONTRATOS

CONFIDENCIAL

fiscal Pensylvania 127 PB, Col. Nápoles CP. 03810 Alcaldía Benito Juárez, CDMX, mismo que señala para los fines y efectos legales de este Convenio.

**4. Declaran conjuntamente las Partes, a través de sus representantes y apoderados legales, que:**

4.1 Manifiestan su conformidad en formalizar el presente **Convenio** con el objeto, entre otros que se describe en el clausulado del presente Convenio, para (i) definir la forma en que combinaran sus esfuerzos, recursos y capacidades, para conjuntamente elaborar y presentar, en tiempo y forma ante la Convocante, una oferta competitiva incluyendo la propuesta técnica y económica en términos de lo establecido en la Convocatoria de la Licitación y de la (s) junta (s) de aclaración (es); (ii) prestarán conjuntamente los servicios descritos en el Contrato de prestación de servicios, que en su caso celebren con la Convocante (el "Contrato de Prestación de Servicios"), con base a lo establecido en el presente Convenio, en las bases de la licitación, conforme a lo dispuesto en los artículos 34 Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("La Ley"), 44 de su Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("Reglamento") y demás disposiciones relativas y aplicables vigentes en la materia.

4.2 Cada una de las **Partes** identifica y se reconocen recíprocamente la personalidad jurídica de las otras **Partes**, así como sus facultades y atribuciones para la celebración del presente **Convenio.**

4.3 Acuerdan de manera libre y voluntaria suscribir el presente **Convenio**, por lo que, en ningún momento presente o futuro, podrán alegar dolo, mala fe o error alguno que anule los efectos y alcances del presente Convenio; en este sentido, las **Partes** se comprometen al fiel y exacto cumplimiento de sus obligaciones que le correspondan, así como aquellas que en su caso adquieran con la **Convocante** con motivo de la Licitación.

4.4. En caso de que resulte adjudicada la presente proposición conjunta en los términos del presente Convenio, se comprometen a formalizar el contrato respectivo de conformidad con las bases, La Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("La Ley"), Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("Reglamento") y demás disposiciones relativas y aplicables vigentes en la materia.

En virtud de las declaraciones que anteceden, las **Partes** acuerdan emitir y obligarse al tenor de las siguientes:

001

## CLÁUSULAS

### PRIMERA. Objeto.

**"LAS PARTES"** convienen en conjuntar sus recursos técnicos, legales y administrativos para presentar una propuesta competitiva en el procedimiento de La Licitación en la que participan, y que en caso de ser adjudicados, se obligan a prestar el **"Servicios Administrados de Seguridad Informática (SASI) 2022-2024"**, (en adelante los "Servicios"), en la forma y términos que se detallan en la propuesta técnica y económica, la cual se tiene aquí por reproducida como si a la letra se insertase, y en los términos que se describen en el Anexo A del presente Convenio, denominado "Matriz de Responsabilidades".

Lo anterior, sin perjuicio de las acciones que sean requeridas entre las **Partes** para el fiel y debido cumplimiento del objeto del presente **Convenio**, así como cualquier obligación que derive del contenido y alcances, según resulte aplicable de las bases, la junta de aclaraciones, La Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("La Ley"), Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("Reglamento") y demás disposiciones relativas y aplicables vigentes en la materia.

Para efectos del cumplimiento del objeto del presente **Convenio**, las **Partes** se obligan a aportar los recursos técnicos, materiales, administrativos, humanos y de cualquier otra naturaleza análoga, necesarios para la presentación de la **Proposición conjunta** en el marco de la **Licitación** convocada por la "La Convocante", atendiendo a las características, términos, condiciones y demás alcances que para tal efecto se establecen para los **"Servicios"**.

Para tal efecto, las **Partes** se obligan desde este momento a adoptar todas las medidas necesarias para la consecución y logro del objeto del presente, implementando en sus mejores prácticas empresariales, comerciales, técnicas, tecnológicas, jurídicas, financieras, económicas y cualquier otra de naturaleza análoga, así como los recursos suficientes y necesarios para el debido cumplimiento de las obligaciones derivadas del presente **Convenio**.

### SEGUNDA. - Descripción de las obligaciones

Con fundamento en el artículo 44, fracción II, inciso d) del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("Reglamento"), las Partes acuerdan que, en el supuesto de resultar adjudicadas de los servicios objeto de la Licitación, cada una de ellas será la encargada y responsable en su totalidad de prestar los servicios objeto del Contrato de Prestación de Servicios, de conformidad con lo establecido a continuación y en forma desglosada como aparece en la matriz de responsabilidades que queda agregada al presente instrumento como Anexo A

**OPERBES, S.A. DE C.V.** se obliga a:

a) Financiar el proyecto y realizar el pago de fianzas

b) Suministrar, proveer y/o entregar servicios profesionales de SOC (Security Operation Center) con personal certificado y procesos certificados en ISO/IEC 20000-1:2018 e ISO/IEC 27001:2013 para la incorporación de los "Servicios Administrados de Seguridad Informática" incluyendo mesa de ayuda, atención de incidentes, operación, administración, reportes, investigación, monitoreo y asistencia al usuario.

ANEXOS
DIVISIÓN DE CONTRATOS

c) Suministrar la totalidad de los equipos y/o licencias de las siguientes soluciones (nuevas y de renovación):
- Firewalls
- IPS
- Anti-denegación de servicios DDoS
- Redes Privadas Virtuales
- Filtrado de Contenido Web
- Filtrado de Contenido de Correo (Antispam)
- Gestión Unificada de Amenazas (UTM)
- Protección de Amenazas Persistentes Avanzadas (APT)
- Ciberinteligencia
- Protección de Redes Inalámbricas

d) Instalar, configurar y poner en funcionamiento la totalidad de los equipos y soluciones descritas en el inciso d) a excepción de la solución de Protección de Amenazas Persistentes Avanzadas (APT) que será realizado por Silent4Business, S.A. de C.V.

e) Adquirir soporte técnico de tercer nivel (por parte de los fabricantes) de los equipos y software descritos en el inciso d).

f) Proveer Soporte Técnico Especializado y reemplazar equipos y/o partes en caso de daño de los equipos y software descritos en el inciso d).

g) Conceder, procurar y/o producir herramientas de software para el SOC, mesa de ayuda y monitoreo.

h) Realizar los servicios siguientes:
- Sistema de Gestión de Seguridad de la Información (SGSI)
- Gestión de Dominios
- Certificados Digitales SSL
- Servicios de Gestión del Cambio en Seguridad de la Información

i) Proveer de personal especializado y certificado para los siguientes roles:
- Administrador del Centro de Operaciones de Seguridad (SOC)
- Administración y Operación de Soluciones y Herramientas Tecnológicas
- Líder de Proyecto
- Operador de la Mesa de Servicio SOC
- Arquitecto Especializado en Redes y Seguridad

**Silent4Business, S.A. de C.V.** se obliga a:

a) Suministrar, proveer y/o entregar servicios profesionales con personal certificado para la incorporación de los "Servicios Administrados de Seguridad Informática" de las soluciones descritas en el inciso b).

b) Suministrar la totalidad de los equipos y/o licencias de las siguientes soluciones (nuevas y de renovación):
- Firewall Especializado en Servicios Web (WAF)
- Firewall Especializado en Base de Datos (DBF)
- Correlación de Eventos
- Borrado Seguro de Información
- Seguridad en dispositivos Móviles
- Gestión de control de acceso para usuarios privilegiados (AAA)
- Servicios de Prevención de Perdida de Información
- Servicio de Antivirus

c) Instalar, configurar y poner en funcionamiento la totalidad de los equipos y soluciones descritas en el inciso b) además de la solución de Protección de Amenazas Persistentes Avanzadas (APT) suministrada por OPERBES, S.A. DE C.V.

d) Adquirir soporte técnico de tercer nivel (por parte de los fabricantes) de los equipos y software descritos en el inciso b).

001

e) Proveer Soporte Técnico Especializado y reemplazar equipos y/o partes en caso de daño de los equipos y software descritos en el inciso b).

f) Proveer de personal especializado y certificado para los siguientes roles:
- Administración y Operación de Soluciones y Herramientas Tecnológicas

**Bufete Empresarial GTI, S.A. de C.V.** se obliga a:

a) Realizar mantenimientos preventivos para las siguientes soluciones:
- Firewalls
- IPS
- Anti-denegación de servicios DDoS
- Redes Privadas Virtuales
- Filtrado de Contenido Web
- Filtrado de Contenido de Correo (Antispam)
- Firewall Especializado en Servicios Web (WAF)
- Firewall Especializado en Base de Datos (DBF)
- Gestión Unificada de Amenazas (UTM)
- Correlación de Eventos
- Protección de Amenazas Persistentes Avanzadas (APT)
- Protección de Redes Inalámbricas
- Gestión de control de acceso para usuarios privilegiados (AAA)
- Servicios de Prevención de Perdida de Información

En caso de que se omita alguna parte del objeto del Contrato, su cumplimiento le corresponderá al Participante A.

La manera en que se exigirá el cumplimiento de las obligaciones de cada una de las partes que integran la presente proposición conjunta, será por conducto del representante común, independientemente del carácter de obligados mancomunados de las Partes, lo anterior con fundamento en el numeral 3.6 de las bases correspondientes a la Licitación. A mayor abundamiento, el proceso será el siguiente:

1. La Convocante comunicará al representante común, conforme el proceso de notificaciones previsto en la Licitación y el Contrato que se formalice, el exigimiento del cumplimiento de las obligaciones.
2. El representante común atenderá el requisito de la Convocante, atendiéndolo conforme los niveles de servicios previstos en el Anexo Técnico correspondiente a la Licitación y el Contrato que en su caso se formalice.

## TERCERA. – Responsabilidad Mancomunada

Con fundamento al artículo 44 fracción II, inciso e), del Reglamento la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("Reglamento") Las **Partes** convienen entre sí en constituirse como **obligados en forma mancomunada** para cumplir con el presente Convenio, aceptando expresamente en responder ante la Convocante por las obligaciones que se deriven del Contrato de Prestación de Servicios que en su caso se formalice de resultar adjudicados.

## CUARTA. - Representante común.

Con fundamento en el artículo 34 de la Ley y 44, fracción II, inciso c), del Reglamento la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("Reglamento") Las **Partes** acuerdan en otorgar poder amplio y suficiente a la persona moral denominada **Operbes S.A. de C.V**, a través de sus apoderados legales, para adquirir a partir de este

001

ANEXOS
DIVISIÓN DE CONTRATOS

Convenio el carácter de **"Representante común"** para atender todo lo relacionado con la Licitación y efectos del procedimiento de la **Licitación** convocada por "La Convocante" incluyendo sin limitar, el acto de presentación de proposiciones, el acto de adjudicación o fallo y cualquier acto relativo con la defensa de la propuesta técnica y económica presentada en forma conjunta, así como en su caso, presentar cualquier tipo de inconformidad.

En virtud de lo anterior, las Partes están de acuerdo en que **OPERBES S.A. de C.V.**, como representante común, sea intermediario entre las Partes y la Convocante y estará facultada para que, en nombre y representación de las demás Partes, presente todos los documentos relacionados con la Proposición Conjunta y realice cualquier tipo de trámite y gestión ante la Convocante relacionados con la Licitación y, en su caso, el Contrato de Prestación de Servicios que se suscriba con la Convocante en caso de resultar adjudicados y la que pudiera resultar de cualquier convenio modificatorio que se suscriba al respecto en términos de La Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("La Ley"), Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("Reglamento") y demás disposiciones relativas y aplicables vigentes en la materia..

De igual manera, y para tal efecto, las Partes señalan como **domicilio común** para oír y recibir notificaciones relacionadas con La Licitación, el domicilio el ubicado Avenida Javier Barros Sierra, número 540, Torre II, piso 6, Colonia Lomas de Santa Fe, Alcaldía de Álvaro Obregón, C.P. 01219, Ciudad de México.

## QUINTA. - Vigencia.

Las Partes convienen en que la vigencia del presente Convenio será la vigencia que se estipule en caso de resultar adjudicados, en el Contrato de Prestación de Servicios que se suscriba con la Convocante y la que pudiera resultar de cualquier convenio modificatorio que se suscriba al respecto en términos de La Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("La Ley"), Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("Reglamento") y demás disposiciones relativas y aplicables vigentes en la materia.

## SEXTA. - Del cobro de facturas.

Las Partes convienen que **OPERBES S.A. de C.V.**, como representante común de la Participación conjunta, será el único facultado para efectuar la facturación y cobranza de los servicios previstos en la presente Licitación y que en caso de ser adjudicados, estén señalados en el Contrato de Prestación de Servicios y de cualquier convenio modificatorio que se suscriba al respecto en términos de La Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("La Ley"), Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público ("Reglamento") y demás disposiciones relativas y aplicables vigentes en la materia.

## SEPTIMA. - Fianza de Cumplimiento de Obligaciones

Con fundamento en lo dispuesto por el artículo 48 fracción II de "La Ley", se establece que para el caso de que nuestra representada sea adjudicada con el "Servicio" materia de la presente Licitación, la fianza de cumplimiento de contrato será a cargo del Participante A, como representante común de la presente participación conjunta.

001

## OCTAVA. - Jurisdicción

Para todo lo relativo a la interpretación y cumplimiento del presente Convenio, las Partes se someten La Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y demás disposiciones relativas y aplicables vigentes en la materia y a la jurisdicción de los Tribunales Federales competentes, renunciando a cualquier otro fuero que por razón de sus domicilios presentes o futuros o por cualquier otra razón pudiere corresponderles.

Leído que fue el presente convenio por las Partes, enteradas de su alcance y efectos legales, lo firman de conformidad en la Ciudad de México, el 30 de septiembre de 2022.

**FIRMAN DE CONFORMIDAD**

**Por "Operbes, S.A. de C.V".**

**Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes**
**Apoderados Legales**

**Por "Silent4Business, S.A. de C.V."**

**Gerardo Garibay Aymes**
**Representante Legal**

**Por "Bufete Empresarial GTI, S.A. de C.V."**

**Juan Luis Pineda González**
**Representante Legal**

**LA PRESENTE HOJA CORRESPONDE AL CONVENIO DE PROPOSICIÓN CONJUNTA QUE, CELEBRAN OPERBES, S.A. DE C.V., SILENT4BUSINESS, S.A. DE C.V. Y BUFETE EMPRESARIAL GTI, S.A. DE C.V. EN EL MARCO DE LA PRESENTE LICITACIÓN CONVOCADA POR EL INSTITUTO MEXICANO DEL SEGURO SOCIAL, CONFORME A LOS TÉRMINOS Y CONDICIONES QUE SE ESTABLECEN EN LAS DIFERENTES SECCIONES DEL PRESENTE DOCUMENTO**

ANEXOS
DIVISIÓN DE CONTRATOS

CONFIDENCIAL

# ANEXO "A"
# "MATRIZ DE RESPONSABILIDADES"
# "Servicios Administrados de Seguridad Informática (SASI) 2022-2024"

| ALCANCE | OPERBES, S.A DE C.V. | SILENT4BUSINESS, S.A. DE C.V. | Bufete Empresarial GTI, S.A. de C.V. |
|---|---|---|---|
| **SERVICIO DE FIREWALL** | | | |
| Renovación Licenciamiento Firewall (Tipo 1, 2, 3 y 4) | X | | |
| Suministro de Firewall (Tipo 4) | X | | |
| Implementación (Instalación, configuración y puesta en funcionamiento) de los equipos de Firewall (Tipo 4) | X | | |
| Licenciamiento Firewall | X | | |
| Mantenimientos preventivos Firewall | | | X |
| Mantenimientos correctivos Firewall | X | | |
| Soporte técnico Firewall | X | | |
| **SERVICIO DE IPS** | | | |
| Renovación Licenciamiento IPS (Tipo 1, 2, 3 y 4) - | X | | |
| Suministro de IPS (Tipo 3) | X | | |
| Implementación (Instalación, configuración y puesta en funcionamiento) de los equipos de IPS (Tipo 3) | X | | |
| Licenciamiento IPS | X | | |
| Mantenimientos preventivos IPS | | | X |
| Mantenimientos correctivos IPS | X | | |
| Soporte técnico IPS | X | | |
| **EQUIPO DE ANTI-DENEGACIÓN DE SERVICIOS DDOS** | | | |
| Renovación Licenciamiento Anti-denegación de servicios DDoS (Tipo 1 y 2) - | X | | |
| Suministro de equipo de Anti-denegación de servicios DDoS (Tipo 2) | X | | |
| Implementación (Instalación, configuración y puesta en funcionamiento) de los equipos de Anti-denegación de servicios DDoS (Tipo 2) | X | | |
| Licenciamiento Anti-denegación de servicios DDoS | X | | |
| Mantenimientos preventivos Anti-denegación de servicios DDoS | | | X |
| Mantenimientos correctivos Anti-denegación de servicios DDoS | X | | |
| Soporte técnico Anti-denegación de servicios DDoS | X | | |
| **REDES PRIVADAS VIRTUALES** | | | |
| Renovación Licenciamiento de Redes Privadas Virtuales. | X | | |
| Suministro de equipo de Redes Privadas Virtuales. | X | | |

001

| | | | |
|---|---|---|---|
| Implementación (Instalación, configuración y puesta en funcionamiento) de los equipos de Redes Privadas Virtuales. | X | | |
| Licenciamiento de Redes Privadas Virtuales. | X | | |
| Mantenimientos preventivos de Redes Privadas Virtuales. | | | X |
| Mantenimientos correctivos de Redes Privadas Virtuales. | X | | |
| Soporte técnico de Redes Privadas Virtuales. | X | | |
| **FILTRADO DE CONTENIDO WEB** | | | |
| Renovación Licenciamiento Filtrado de Contenido Web | X | | |
| Mantenimientos preventivos de Filtrado de Contenido Web . | | | X |
| Mantenimientos correctivos de Filtrado de Contenido Web . | X | | |
| Soporte técnico de Filtrado de Contenido Web. | X | | |
| **FILTRADO DE CONTENIDO DE CORREO (ANTISPAM)** | | | |
| Renovación Licenciamiento Filtrado de Contenido de Correo (Antispam) | X | | |
| Mantenimientos preventivos de Filtrado de Contenido de Correo (Antispam). | | | X |
| Mantenimientos correctivos de Filtrado de Contenido de Correo (Antispam). | X | | |
| Soporte técnico de Filtrado de Contenido de Correo (Antispam). | X | | |
| **SERVICIOS WEB (WAF)** | | | |
| Renovación Licenciamiento de Servicios Web (WAF) | | X | |
| Suministro de Servicios Web (WAF). | | X | |
| Implementación (Instalación, configuración y puesta en funcionamiento) de los equipos de Servicios Web (WAF) | | X | |
| Licenciamiento de Servicios Web (WAF). | | X | |
| Mantenimientos preventivos de Servicios Web (WAF). | | | X |
| Mantenimientos correctivos de Servicios Web (WAF). | | X | |
| Soporte técnico de Servicios Web (WAF). | | X | |
| **FIREWALL ESPECIALIZADO EN BASE DE DATOS (DBF)** | | | |
| Renovación Licenciamiento de Firewall Especializado en Base de Datos (DBF) | | X | |
| Suministro de Firewall Especializado en Base de Datos (DBF) | | X | |
| Implementación (Instalación, configuración y puesta en funcionamiento) de los equipos de Firewall Especializado en Base de Datos (DBF) | | X | |
| Licenciamiento de Firewall Especializado en Base de Datos (DBF) | | X | |
| Mantenimientos preventivos de Firewall Especializado en Base de Datos (DBF) | | | X |
| Mantenimientos correctivos de Firewall Especializado en Base de Datos (DBF) | | X | |
| Soporte técnico de Firewall Especializado en Base de Datos (DBF) | | X | |

ANEXOS
DIVISIÓN DE CONTRATOS

| | | | |
|---|---|---|---|
| **GESTIÓN UNIFICADA DE AMENAZAS (UTM)** | | | |
| Renovación Licenciamiento de Gestión Unificada de Amenazas (UTM) (Tipo 1, 2, 3, 4) | X | | |
| Suministro de equipos de Gestión Unificada de Amenazas (UTM) (Tipo 4) | X | | |
| Implementación (Instalación, configuración y puesta en funcionamiento) de los equipos de Gestión Unificada de Amenazas (UTM) (Tipo 4) | X | | |
| Licenciamiento de Gestión Unificada de Amenazas (UTM) | X | | |
| Mantenimientos preventivos de Gestión Unificada de Amenazas (UTM) | | | X |
| Mantenimientos correctivos de Gestión Unificada de Amenazas (UTM) | X | | |
| Soporte técnico de Gestión Unificada de Amenazas (UTM) | X | | |
| **CORRELACIÓN DE EVENTOS** | | | |
| Suministro de equipos de Correlación de Eventos | | X | |
| Implementación (Instalación, configuración y puesta en funcionamiento) de los equipos de Correlación de Eventos | | X | |
| Licenciamiento de Correlación de Eventos | | X | |
| Mantenimientos preventivos de Correlación de Eventos | | | X |
| Mantenimientos correctivos de Correlación de Eventos | | X | |
| Soporte técnico de Correlación de Eventos | | X | |
| **PROTECCIÓN DE AMENAZAS PERSISTENTES AVANZADAS (APT)** | | | |
| Suministro de equipos de Protección de Amenazas Persistentes Avanzadas (APT) | X | | |
| Implementación (Instalación, configuración y puesta en funcionamiento) de los equipos de Protección de Amenazas Persistentes Avanzadas (APT) | X | X | |
| Licenciamiento de Protección de Amenazas Persistentes Avanzadas (APT) | X | | |
| Mantenimientos preventivos de Protección de Amenazas Persistentes Avanzadas (APT) | | | X |
| Mantenimientos correctivos de Protección de Amenazas Persistentes Avanzadas (APT) | X | | |
| Soporte técnico de Protección de Amenazas Persistentes Avanzadas (APT) | X | | |
| **SUMINISTRO DE BORRADO SEGURO DE INFORMACIÓN** | | X | |
| **SUMINISTRO DE CIBERINTELIGENCIA** | X | | |
| **PROTECCIÓN DE REDES INALÁMBRICAS Y SEGURIDAD EN DISPOSITIVOS MÓVILES** | | | |
| Suministro de equipos y licencias de Gestión de control de Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles | X | X | |
| Implementación (Instalación, configuración y puesta en funcionamiento) de los equipos y | X | X | |

CONFIDENCIAL

002

| | | | |
|---|---|---|---|
| licencias de Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles | | | |
| Licenciamiento de Gestión de control de Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles | X | X | |
| Mantenimientos preventivos de Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles | | | X |
| Mantenimientos correctivos de Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles | X | X | |
| Soporte técnico de Protección de Gestión de Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles | X | X | |
| **GESTIÓN DE CONTROL DE ACCESO PARA USUARIOS PRIVILEGIADOS (AAA)** | | | |
| Suministro de equipos de Gestión de control de acceso para usuarios privilegiados (AAA) | | X | |
| Implementación (Instalación, configuración y puesta en funcionamiento) de los equipos de Gestión de control de acceso para usuarios privilegiados (AAA) | | X | |
| Licenciamiento de Gestión de control de acceso para usuarios privilegiados (AAA) | | X | |
| Mantenimientos preventivos y correctivos de Gestión de control de acceso para usuarios privilegiados (AAA) | | | X |
| Soporte técnico de Protección de Gestión de control de acceso para usuarios privilegiados (AAA) | | X | |
| **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)** | X | | |
| **SUMINISTRO DE GESTIÓN DE DOMINIOS** | X | | |
| **SUMINISTRO DE CERTIFICADOS DIGITALES SSL** | X | | |
| **SUMINISTRO DE SERVICIOS DE PREVENCIÓN DE PERDIDA DE INFORMACIÓN** | | X | |
| Suministro de equipos y licencias de Prevención de Pérdida de Información | | X | |
| Implementación (Instalación, configuración y puesta en funcionamiento) de los equipos y licencias de Prevención de Pérdida de Información | | X | |
| Licenciamiento de Prevención de Pérdida de Información | | X | |
| Mantenimientos preventivos y correctivos de Prevención de Pérdida de Información | | | X |
| Soporte técnico de Prevención de Pérdida de Información | | X | |
| **SERVICIO DE ANTIVIRUS** | | | |
| Suministro de licencias de Antivirus | | X | |
| Implementación (Instalación, configuración y puesta en funcionamiento) de las licencias de Servicio de Antivirus | | X | |
| Mantenimientos correctivos de licencias Protección de Servicio de Antivirus | | X | |

ANEXOS
DIVISIÓN DE CONTRATOS

| | | | |
|---|---|---|---|
| Soporte técnico de Protección de Servicio de Antivirus | | X | |
| **SUMNISTRO DE SERVICIOS DE GESTIÓN DEL CAMBIO EN SEGURIDAD DE LA INFORMACIÓN** | X | | |
| **SUMNISTRO SERVICIOS DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)** | X | | |
| **CAMBIO DE SOLUCIÓN DE LA INFRAESTRUCTURA EXISTENTE A EQUIPAMIENTO NUEVO** | | | |
| Suministro de equipamiento nuevo para sustitución del existente:<br>- Firewall Tipo 1, 2, 3 y 4<br>- IPS Tipo 1,2,3 y 4,<br>- Anti-denegación de servicios DDoS Tipo 1 y 2,<br>- Redes Privadas Virtuales,<br>- Gestión Unificada de Amenazas (UTM) Tipo 1, 2, 3 y 4 | X | | |
| Implementación (Instalación, configuración y puesta en funcionamiento) de los equipos de equipamiento nuevo para sustitución del existente:<br>- Firewall Tipo 1, 2, 3 y 4<br>- IPS Tipo 1,2,3 y 4,<br>- Anti-denegación de servicios DDoS Tipo 1 y 2,<br>- Redes Privadas Virtuales,<br>- Gestión Unificada de Amenazas (UTM) Tipo 1, 2, 3 y 4 | X | | |
| Licenciamiento de equipamiento nuevo para sustitución del existente:<br>- Firewall Tipo 1, 2, 3 y 4<br>- IPS Tipo 1,2,3 y 4,<br>- Anti-denegación de servicios DDoS Tipo 1 y 2,<br>- Redes Privadas Virtuales,<br>- Gestión Unificada de Amenazas (UTM) Tipo 1, 2, 3 y 4 | X | | |
| Mantenimientos preventivos de equipamiento nuevo para sustitución del existente:<br>- Firewall Tipo 1, 2, 3 y 4<br>- IPS Tipo 1,2,3 y 4,<br>- Anti-denegación de servicios DDoS Tipo 1 y 2,<br>- Redes Privadas Virtuales,<br>- Gestión Unificada de Amenazas (UTM) Tipo 1, 2, 3 y 4 | | | X |
| Mantenimientos preventivos y correctivos de equipamiento nuevo para sustitución del existente:<br>- Firewall Tipo 1, 2, 3 y 4<br>- IPS Tipo 1,2,3 y 4,<br>- Anti-denegación de servicios DDoS Tipo 1 y 2,<br>- Redes Privadas Virtuales, | X | | |

UNIDENCIAL

| | | | |
|---|---|---|---|
| - Gestión Unificada de Amenazas (UTM) Tipo 1, 2, 3 y 4 | | | |
| Soporte técnico de Protección de Servicio de equipamiento nuevo para sustitución del existente:<br>- Firewall Tipo 1, 2, 3 y 4<br>- IPS Tipo 1,2,3 y 4,<br>- Anti-denegación de servicios DDoS Tipo 1 y 2,<br>- Redes Privadas Virtuales,<br>- Gestión Unificada de Amenazas (UTM) Tipo 1, 2, 3 y 4 | X | | |
| **MESA DE SERVICIO SOC** | | | |
| Atención a solicitudes de servicio e incidentes | X | | |
| Soporte técnico. | X | X | |
| Soporte técnico en sitio. | X | X | |
| Servicios de mantenimiento. | X | X | |
| Mantenimiento preventivo | | X | X |
| Mantenimiento correctivo. | X | X | |
| **PERFIL DEL PROVEEDOR** | | | |
| Administrador del Centro de Operaciones de Seguridad (SOC) | X | | |
| Administración y Operación de Soluciones y Herramientas Tecnológicas | X | X | |
| Líder de Proyecto | X | | |
| Operador de la Mesa de Servicio SOC | X | | |
| Arquitecto Especializado en Redes y Seguridad | X | | |
| **ENTREGABLES GENERALES** | X | X | |
| **ENTREGABLES BAJO DEMANDA** | X | | |
| **ENTREGABLES PERIÓDICOS** | X | | |
| **FACTURACIÓN DE LOS SERVICIOS.** | X | | |
| **COBRANZA DE LOS SERVICIOS.** | X | | |

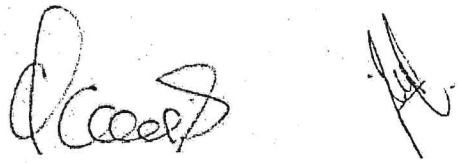
ANEXOS
DIVISIÓN DE CONTRATOS



00

## FIRMAN DE CONFORMIDAD

**Por "Operbes, S.A. de C.V".**



**Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes**

**Apoderados Legales**

**Por "Silent4Business, S.A. de C.V."**



**Gerardo Garibay Aymes**
**Representante Legal**

**Por "Bufete Empresarial GTI, S.A. de C.V."**



**Juan Luis Pineda González**
**Representante Legal**

**LA PRESENTE HOJA CORRESPONDE AL CONVENIO DE PROPOSICIÓN CONJUNTA QUE, CELEBRAN OPERBES, S.A. DE C.V., SILENT4BUSINESS, S.A. DE C.V. Y BUFETE EMPRESARIAL GTI, S.A. DE C.V. EN EL MARCO DE LA PRESENTE LICITACIÓN CONVOCADA POR EL INSTITUTO MEXICANO DEL SEGURO SOCIAL, CONFORME A LOS TÉRMINOS Y CONDICIONES QUE SE ESTABLECEN EN LAS DIFERENTES SECCIONES DEL PRESENTE DOCUMENTO.**

CONFIDENCIAL

0023