

The image features a large, semi-transparent watermark of the IMSS logo in the background. The logo consists of a stylized eagle with its wings spread, perched on a cactus, all enclosed within a rounded square border. Below the eagle, the letters 'IMSS' are written in a bold, sans-serif font.

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



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

CONTRATO
NÚMERO
019E18222-002

CONTRATO ABIERTO PLURIANUAL PARA LA PRESTACIÓN DE LOS "SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA (SASI) 2022-2024" (PARTIDA 2), 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 **CONSULTING ALL SERVICE IN TELECOM AND MEDICE, S. DE R.L. DE C.V.**, (EL PARTICIPANTE A) REPRESENTADA POR EL **C. JULIO CRUZ GÓMEZ**, EN SU CARÁCTER DE REPRESENTANTE LEGAL, EN PARTICIPACIÓN CONJUNTA CON **SECURE LABS, S.A. DE C.V.** (EL PARTICIPANTE B), REPRESENTADA POR LOS **C.C. ALBERTO VARGAS MAGAÑA Y FRANCISCO OVALLE FELIX**, EN SU CARÁCTER DE REPRESENTANTES LEGALES Y **BOHMER STRATEGISTS, S. DE R.L. DE C.V.** (EL PARTICIPANTE C), REPRESENTADA POR EL **C. ISIDORO GUILLERMO HERNÁNDEZ ZAGACETA**, 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:

ANTECEDENTE

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.

DECLARACIONES

- 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

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

Página 1

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



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

CONTRATO
NÚMERO
019E18222-002

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.

- 1.4 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.
- 1.5 “**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 0000439260-2022, 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)**.
- 1.6 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)**.
- 1.7 Para efectos fiscales las Autoridades Hacendarias le han asignado el Registro Federal de Contribuyentes N° **IMS421231145**.
- 1.8 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.

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

DIVISIÓN DE CONTRATOS
 NIVEL CENTRAL

Dirección Jurídica
 Unidad de Asesoría Jurídica
 de Atención y Organización Institucional
 Coordinación de Organización y Consulta

La validación jurídica se efectuó sin prejuicio sobre la justificación, el procedimiento, el cumplimiento de los requisitos, la idoneidad de la prestación de la investigación de mercado, correspondiente, ni se pronuncia sobre la procedencia y/o viabilidad de las acciones técnicas, administrativas, financieras, presupuestales, de planeación, de programación, de ejecución, de seguimiento y de evaluación, ni sobre los demás requisitos, técnicos y/o contractuales.

Los aspectos jurídicos del presente documento han sido validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 de la Ley del Seguro Social, y el artículo 10 de la Ley del Seguro Popular, y se basa en el dictamen elaborado por la División de Dictamen Jurídico de Contratos y Compras, de la Dirección de Administración y Organización Institucional, en cumplimiento de las facultades conferidas en el artículo 10 de la Ley del Seguro Social, y el artículo 10 de la Ley del Seguro Popular, bajo el número: DGDDCC/ADG/2022/005



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

CONTRATO
NÚMERO
019E18222-002

II.- “EL PROVEEDOR” declara, a través de sus Representantes Legales, que:

CONSULTING ALL SERVICE IN TELECOM AND MEDICE, S. DE R.L. DE C.V., (El Participante A)

- II.1** Es una persona moral legalmente constituida según consta en la Escritura Pública número 268,140 de fecha 06 de noviembre de 2012, pasada ante la fe del Licenciado Claudio Juan Ramón Hernández de Rubín, Titular de la Notaría Pública número 123 del Distrito Federal, hoy Ciudad de México, actuando como asociado en el protocolo de la Notaría número 6 de la que es titular el Licenciado Fausto Rico Álvarez e inscrita en el Registro Público de la Propiedad y de Comercio de la misma Entidad, en el folio mercantil electrónico número 483484-1, denominada **CONSULTING ALL SERVICE IN TELECOM AND MEDICE, S. DE R.L. DE C.V.**, cuyo objeto social es, entre otros, la prestación de todo tipo de servicios públicos de telecomunicaciones y/o radiodifusión previa concesión, autorización, o similar que en caso otorgue el Instituto Federal de Telecomunicaciones y/o cualquier autoridad competente; la instalación, operación, explotación o comercialización de una red pública de telecomunicaciones.
- II.2** El C. Julio Cruz Gómez, 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 31,188 de fecha 20 de octubre de 2016, pasada ante la fe del Licenciado Pedro Bernardo Barrera Cristiani, Titular de la Notaría Pública número 82 de la 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 483484-1, mismo que bajo protesta de decir verdad manifiesta que no le 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 Adquisiciones
Coordinación de Planeación y Contratos

La validación jurídica se efectúa sin prejuzgar sobre la licitud, procedencia, términos y condiciones de la contratación, ni del cumplimiento de los requisitos de fondo y forma, sino que se pronuncia sobre la procedencia y/o posibilidad de las acciones jurídicas y/o administrativas que determine el órgano competente de la instancia.

Los aspectos jurídicos del presente documento fueron validados por la sección titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 del Reglamento de Organización y Funciones de la Secretaría de Economía, en el marco de la coordinación de la Unidad de Adquisiciones, Arrendamientos y Servicios del Sector Público, bajo el número de expediente: 02/019E18222/002/02/005

GOBIERNO DE
MÉXICO



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

CONTRATO
NÚMERO
019E18222-002

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 **CAS1211066S3**.

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 calle Rio Rhin número 22, Interior 504, Colonia Cuauhtémoc, Demarcación Territorial Cuauhtémoc, Código Postal 06500, Ciudad de

Dirección Jurídica
 de Atención a Organismos 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 cumplimiento de las obligaciones de las partes, sino para verificar que se promueva sobre la precedencia y/o prioridad de las partes del mismo, en el momento de la suscripción del presente instrumento jurídico, conforme a la Ley del Procedimiento de Adquisición, a la Ley del Registro de Empresas y Proveedores, al Reglamento de la Ley del Registro de Empresas y Proveedores, al Reglamento de la Ley de Acceso a la Información Pública y al Reglamento de la Ley de Transparencia, en sus disposiciones aplicables. En consecuencia, se registra bajo el número: 019E18222/002/02/2025

GOBIERNO DE MEXICO
 INSTITUTO MEXICANO DEL SEGURO SOCIAL



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

CONTRATO
NÚMERO
019E18222-002

México, teléfono: 5554552055, correo electrónico: julio.cruz@callit.com.mx

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.

SECURE LABS, S.A. DE C.V. (El Participante B)

II.13 Es una persona moral legalmente constituida según consta en la Escritura Pública número 122,833 de fecha 23 de enero de 2020, pasada ante la fe del Licenciado Othón Pérez Fernández del Castillo, Titular de la Notaría Pública número 63 de la Ciudad de México, e inscrita en el Registro Público de Comercio de la misma Entidad, en el folio mercantil electrónico número N-2020018436, denominada **SECURE LABS, S.A. DE C.V.**, cuyo objeto social es, entre otros, elaboración, compra, venta, distribución, comercialización, implantación, desarrollo, ejecución y en general llevar a cabo todo tipo de actividades relacionadas con programas de computación, sistemas de información, servicios tecnológicos de seguridad, sistemas de animación digital, implantación de lenguajes y redes para computadoras y cualquier tipo de medios electrónicos, así como el establecimiento de sitios electrónicos, incluyendo aquellos accesibles vía redes de comunicación incluyendo, entre otros, el Internet; importación y exportación de programas, sistemas de información, sistemas de comunicación y redes de computadoras.

II.14 Los C.C. Alberto Vargas Magaña y Francisco Ovalle Felix, 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 122,833 de fecha 23 de enero de 2020, pasada ante la fe del Licenciado Othón Pérez Fernández del Castillo, Titular de la Notaría Pública número 63 de la Ciudad de México, e inscrita en el Registro Público de Comercio de la misma Entidad, en el folio mercantil electrónico número N-2020018436, mismo que bajo protesta de decir verdad manifiestan que no les 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.

En caso de que **“EL PROVEEDOR”** se encuentre en los supuestos señalados anteriormente, el contrato será nulo previa determinación de la autoridad competente de

Dirección Jurídica
 Unidad de Asesoría Legal
 de Atención a Organismos Fiscalizadores y
 Coordinación de Legislación y Consulta
 La validación jurídica se efectuó sin prejuicio sobre la justificación,
 procedimiento, términos y condiciones de la contratación, ni en
 materia de responsabilidad por el cumplimiento de la obligación,
 prelación sobre la procedencia y/o prioridad de las acciones técnicas
 de ejecución de los contratos, ni en materia de determinación procedente
 las áreas de registro, electrónica y documentación.
 Los aspectos jurídicos del presente documento fueron validados por la serena
 titular de la Dirección Jurídica, el cumplimiento a lo dispuesto en el artículo 75
 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público,
 en el momento de su elaboración por la División de Contratos y
 Compras, en el momento de su inscripción en el Registro Público de Comercio
 de la Ciudad de México, y en el momento de su inscripción en el
 Registro Público de Comercio de la misma Entidad, en consecuencia, se registra
 bajo el número: 642/2020/12/23/2020



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

CONTRATO
NÚMERO
019E18222-002

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 **SLA2001239H9**.

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"**.

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



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

**CONTRATO
NÚMERO
019E18222-002**

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 calle San Jacinto número 8, Departamento A, Colonia San Ángel, Demarcación Territorial Álvaro Obregón, Código Postal 01000, Ciudad de México, teléfono: 55 8525 4111, correo electrónico: alberto.vargas@secnesys.com.mx
- 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.

BOHMER STRATEGISTS, S. DE R.L. DE C.V. (El Participante C)

- II.25** Es una persona moral legalmente constituida según consta en la Póliza número 1,971 de fecha 01 de marzo de 2021, pasada ante la fe del Licenciado Carlos Luviano Montelongo, Titular de la Correduría Pública número 64 de la Plaza del Estado de Jalisco, e inscrita en el Registro Público de Comercio de la misma Entidad, en el folio mercantil electrónico número N-2021021629, denominada **BOHMER STRATEGISTS, S. DE R.L. DE C.V.**, cuyo objeto social es, entre otros, comprar, vender y en general comercializar toda clase de bienes, productos o servicios; comercialización, compra, venta, importación, exportación, industrialización, distribución, fabricación, representación, concesión, comisión, arrendamiento de toda clase de bienes, productos, servicios y servicios secundarios de valor agregado y el comercio en general con toda clase de equipos, servicios y productos.

- II.26** El C. Isidoro Guillermo Hernández Zagaceta, 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 947 de fecha 17 de octubre de 2022, pasada ante la fe del Licenciado Gabriel Villalever García de Quevedo, Titular de la Notaría Pública número 04 de Tonalá, Jalisco, mismo que bajo protesta de decir verdad manifiesta que no le han sido limitado ni revocado en forma alguna.

- 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.

Dirección Jurídica
Unidad de Adquisiciones y
de Atención a Organismos Fiscalizadores
y
Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin perjuicio sobre la justificación, el procedimiento, el término y las condiciones de la contratación, ni del cumplimiento de los requisitos de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en materia de los aspectos técnicos, económicos, financieros, administrativos, legales y demás que determinan los procedimientos de adquisición de bienes, productos o servicios, en su caso, en los términos de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 25 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en base en el dictamen elaborado por la División de Dictámenes Jurídicos de Contratos y Compras, en el expediente de Adquisiciones y Organismos Fiscalizadores. En consecuencia, se registra bajo el número: 019E18222/002/2022/005





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

CONTRATO
NÚMERO
019E18222-002

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 **BST2103235Z1**.

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

[Handwritten signatures in blue ink]

GOBIERNO DE MÉXICO
 DISEÑO: ROSALBA ESCOBAR
 DIRECCIÓN DE ADMINISTRACIÓN
 DE FISCALIDAD, CONTRATACIÓN Y SERVICIOS
 CONVENIO 138 DE LA OIT
 VALIDACIÓN JURÍDICA DE DOCUMENTOS
 El presente documento fue validado por la persona titular de la Dirección Jurídica en cumplimiento a lo establecido en el artículo 26 del Reglamento de la Ley del Seguro Social, con base en el dictamen elaborado por la División de Dictámenes Jurídicos de Contratos y Conciliación de la Dirección de Administración y Organismo Fiscalizadores. En consecuencia, se registra bajo el número: DD01DDCA02020001



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

CONTRATO
NÚMERO
019E18222-002

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 Guanajuato número 224, Piso 2, Despacho 205, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, Ciudad de México, teléfonos: 5550682170 y 557190744, correo electrónico: consultoria@bohmerstrategists.com
- 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:

CLÁUSULAS

PRIMERA. OBJETO DEL CONTRATO.

"EL PROVEEDOR" acepta y se obliga a proporcionar a "EL INSTITUTO" los "Servicios Administrados de Seguridad Informática (SASI) 2022-2024" (Partida 2), al amparo del procedimiento de contratación señalado en el antecedente de este instrumento jurídico.



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

CONTRATO
 NÚMERO
 019E18222-002

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"

SEGUNDA. DE LOS MONTOS Y PRECIOS.

El monto mínimo del presente contrato es por la cantidad de **\$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 (I.V.A.), y el monto máximo del mismo es por la cantidad de **\$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 (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:

MONTOS	PARTIDA 2			TOTAL
	AÑO			
	2022	2023	2024	
IMPORTE MÁXIMO INCLUYENDO IVA	\$5,685,205.63	\$22,740,822.50	\$17,055,616.88	\$45,481,645.01
IMPORTE MÍNIMO INCLUYENDO IVA	\$2,274,082.25	\$9,096,329.00	\$6,822,246.75	\$18,192,658.00

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 2), por lo que **"EL PROVEEDOR"** no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.

GOBIERNO DE MEXICO
 Dirección Jurídica
 Unidad de Atención a Ciudadanos Fiscalizadora
 de Atención a Ciudadanos y Consulta
 La validación jurídica de este documento tiene validez por la presencia
 de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75
 del Reglamento Interior del Instituto Mexicano del Seguro Social, y en
 base en el dictamen elaborado por la Unidad de Dictámenes Jurídicos de
 Consulta y de Atención a Ciudadanos Fiscalizadora, en consecuencia, se
 declara válido el presente documento. En consecuencia, se reglamos
 bajo el número 0018222/019E/2022



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

CONTRATO
NÚMERO
019E18222-002

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 Trámite 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.

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.

Dirección Jurídica
Asesoría y
Coordinación a Organos Ejecutivos y
Coordinación a Legales y Consulta

La validación jurídica se efectúa en prelación sobre la justificación, procedimientos, términos y condiciones de la contratación, ni del contrato, ni de los documentos que forman parte del expediente, ni de la promesa sobre la procedencia y/o viabilidad de los aspectos técnicos, económicos y financieros, y las circunstancias que determinaron procedimientos de selección y/o contratación.

Los aspectos jurídicos del presente documento tienen validez por la misma titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en base en el dictamen elaborado por la División de Dictamen Jurídico de Contratos y Compras y de Atención a Clientes y Planeación. En caso contrario, se regirán bajo el número de Dictamen de Disponibilidad Presupuestal.



B
J
A
B
X



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

CONTRATO
NÚMERO
019E18222-002

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 IMS421231145 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, si no se ha determinado, calculado y notificado a **“EL PROVEEDOR”** las penas convencionales o deducciones pactadas en el presente contrato, así como su registro y validación en el Sistema PREI Millenium.

“EL PROVEEDOR” podrá optar por cobrar a través de factoraje financiero conforme al Programa de Cadenas Productivas de Nacional Financiera, S.N.C., Institución de Banca de Desarrollo con **“EL INSTITUTO”**.

En caso de que **“EL PROVEEDOR”** reciba pagos en exceso deberá reintegrar las cantidades pagadas en exceso más los intereses correspondientes, conforme a la tasa que establezca la Ley de Ingresos de la Federación, en los casos de prórroga para el pago de créditos fiscales. Los intereses se calcularán sobre las cantidades en exceso y se computarán por días naturales



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

CONTRATO
NÚMERO
019E18222-002

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.

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

GOBIERNO DE MÉXICO
Dirección Jurídica
Unidad de Asesoría Consultiva y
Coordinación de Legislación Consultiva
La validación jurídica de este acto se otorga al participar sobre la justificación, procedimientos, términos y condiciones de la contratación, el del presente contrato, en el portal de servicios a proveedores, el cual se encuentra en el portal de servicios a proveedores de la página de "EL INSTITUTO".
Los aspectos jurídicos del presente documento son válidos por la presente en el portal de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 15 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y en base a lo dictaminado por la Dirección de Asesoría Jurídica de Contratos y Compras de la Coordinación de Legislación y Consulta, de la Unidad de Asesoría Consultiva y Coordinación de Legislación Consultiva, en cumplimiento de lo dispuesto en el artículo 15 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, bajo el número de expediente 02/019E18222/002/002.



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

CONTRATO
NÚMERO
019E18222-002

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 **“CONSULTING ALL SERVICE IN TELECOM AND MEDICE, S. DE R.L. DE C.V.”**, en la que se efectuará la transferencia electrónica de pago.

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

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

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

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

Dirección Jurídica y
Asesoría a Organizaciones
Facilitadora y
Coordinación de Legislación y Consulta

La validación jurídica se efectuó en preludio a la identificación, procedimientos, términos y condiciones de la contratación, al del presente contrato, así como a la propuesta de la actividad de los aspectos técnicos, económicos y legales, para determinar si los mismos se determinaron procedentes en el presente contrato.

Los aspectos jurídicos del presente documento han sido validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, de conformidad con el Convenio de la Coordinación de Legislación y Consulta, de la Unidad de Adquisiciones, Arrendamientos y Servicios del Sector Público, de conformidad con el número de registro 09/03/2016.





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

CONTRATO
NÚMERO
019E18222-002

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 Modificadorio, 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 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.

La validación jurídica se efectúa de acuerdo al protocolo de validación jurídica, el cual se encuentra en el expediente de contratación, en el cual se detallan las acciones que se deben realizar para la validación jurídica, en el momento de la contratación, al momento de la ejecución del contrato y al momento de la cancelación del contrato, de acuerdo a lo establecido en el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Los aspectos jurídicos del presente documento han sido validados por la persona titular de la Dirección Jurídica, de conformidad con el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en el momento de la contratación, al momento de la ejecución del contrato y al momento de la cancelación del contrato, de acuerdo a lo establecido en el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

El presente documento fue elaborado por la Unidad de Adquisiciones, de la Dirección de Administración, del Instituto Mexicano del Seguro Social, en el momento de la contratación, al momento de la ejecución del contrato y al momento de la cancelación del contrato, de acuerdo a lo establecido en el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.



“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”.

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

Dirección Jurídica
 de Atención a Organismos Fiscalizadores
 Coordinación de Legitimación y Consulta

La validación jurídica se efectúa sin perjuicio sobre la justificación, procedencia, términos, condiciones de la contratación, ni el procedimiento de selección, el cual es de competencia de la instancia correspondiente y/o la autoridad competente para la determinación procedente, en su caso, de conformidad con lo establecido en el artículo 107 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. En consecuencia, se registró bajo el número 0470102/2019.

Los aspectos jurídicos del presente documento fueron validados por la instancia de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en el Distrito Federal, por la División de Contratos y Servicios del Sector Público, en el Distrito Federal, en el Estado de México, en el Estado de Guerrero y de Atención a Organismos Fiscalizadores. En consecuencia, se registró bajo el número 0470102/2019.





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

CONTRATO
 NÚMERO
 019E18222-002

- 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 solidaria 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)**.

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.

Dirección Jurídica
 de Adquisiciones, Contratos, Ejecución y
 Coordinación de Legislación y Consulta
 La validación jurídica se efectuó sin perjuicio sobre la justificación
 procedimental, términos y condiciones de la contratación, ni del
 cumplimiento de los requisitos de la convocatoria, así como de la
 presencia sobre la procedencia y/o utilidad de los aspectos técnicos,
 económicos y las características de los bienes o servicios que se
 adquieren, así como de la oportunidad de la adquisición.
 Los aspectos jurídicos del presente documento fueron validados por la asesora
 titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75
 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del
 Sector Público, en el Estado de México, en la División de Contratos y Ejecución
 de los Contratos, de la Dirección de Adquisiciones, Contratos, Ejecución y
 Coordinación de Legislación y Consulta, el día 28 de septiembre de 2024.
 Bajo el número: 18/2024/OA/OA/002/2024





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

CONTRATO
 NÚMERO
 019E18222-002

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

Dirección Jurídica
 Unidad de Atención a Oligos FISCALIZACIÓN
 Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin perjuicio sobre la justificación, procedimiento, términos y condiciones de la contratación, o de la promoción sobre la procedencia y/o validez de los aspectos técnicos, económicos y financieros que se determinan en el procedimiento, en la forma que se establezca, en el momento de la contratación.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, de conformidad con el artículo 75 del Reglamento de Organización y Funciones de la División de Contratos y Compras, en el momento de la contratación, en el momento de la firma del presente documento. En consecuencia, se registra bajo el número de validación de la División de Contratos y Compras.



GOBIERNO DE
 MÉXICO

Handwritten signature/initials

Handwritten signature/initials

Handwritten signature/initials



"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.

DÉCIMA QUINTA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES.

Vertical text on the left margin including 'GOBIERNO DE MÉXICO' and 'Dirección Jurídica'.



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

CONTRATO
 NÚMERO
 019E18222-002

“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 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

Dirección Jurídica
 Unidad de Atención al Ciudadano Fiscalizadora
 Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin perjuicio de la justificación, procedimiento, términos y condiciones de la contratación, ni se pronuncia sobre la procedencia y/o viabilidad de los aspectos técnicos, económicos, financieros, administrativos, de cumplimiento de requisitos, licitación y/o contratación.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, y su consentimiento a lo dispuesto en el artículo 75 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, se basa en el dictamen elaborado por la División de Dictamen Jurídico de Contratos y Servicios del Sector Público, en el expediente de validación de los aspectos jurídicos, Condiciones y de Materiales, y/o de Pliego de Especificaciones, en consecuencia, se registró bajo el número 067010102/07/2022/005.





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

CONTRATO
 NÚMERO
 019E18222-002

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”.

Quando 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.

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.

Dirección Jurídica
 Unidad de Asesoría Consultiva y
 Coordinación de Legislación y Consulta
 La validación jurídica se efectúa sin perjuicio de la validez, eficacia, términos, condiciones de la contratación, ni de
 los efectos de la misma, en el caso de que se produzca un acto de corrupción, fraude, o cualquier otro acto ilícito que
 promueva o favorezca la realización de la contratación económica y las demás circunstancias que determinen presencias
 de una irregularidad, inequidad y/o corrupción.
 Los aspectos jurídicos del presente instrumento fueron validados por la asesora
 titular de la Dirección Jurídica, de conformidad con lo dispuesto en el artículo 75
 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y
 en el artículo 10 del Reglamento de la Ley de Adquisiciones, Arrendamientos y
 Servicios del Sector Público, emitido por el Director de Asesoría Jurídica de Contratos
 y Compras, de la Coordinación de Adquisición de Bienes y Contratación de Servicios,
 de la Unidad de Asesoría Consultiva y Coordinación de Legislación y Consulta, de la
 Dirección de Administración, del Instituto Mexicano del Seguro Social, en
 base en el documento elaborado por el Director de Asesoría Jurídica de Contratos
 y Compras, de la Coordinación de Adquisición de Bienes y Contratación de Servicios,
 bajo el número: 04/0181/2017/ADQUISICIONES

GOBIERNO DE
 MÉXICO





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

CONTRATO
 NÚMERO
 019E18222-002

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, 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)**.

Dirección Jurídica
 Unidad de Asesoría y Organización Consultiva
 de Adquisición y Organización Consultiva

La validación jurídica se efectúa sin perjuicio de la justificación, procedimiento, términos y condiciones de la contratación, ni del pronunciamiento sobre la procedencia y/o viabilidad de los aspectos técnicos, económicos, financieros, administrativos, de cumplimiento de requisitos, de las áreas requeridas, técnica y/o sustantiva.

Los aspectos jurídicos del presente documento han sido validados por la persona titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 75 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y en base en el dictamen elaborado por la División de Dictamen Jurídico de Contratos y Compras de Bienes, Servicios y Obras, de la Unidad de Asesoría y Organización Consultiva de Adquisición y Organización Consultiva. En consecuencia, se registra bajo el número de expediente 019E18222-002.





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

CONTRATO
NÚMERO
019E18222-002

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.

VIGÉSIMA SEGUNDA. SANCIONES APLICABLES Y TERMINACIÓN DE LA RELACIÓN CONTRACTUAL

Dirección Jurídica
 División de Contratos y
 Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin perjuicio de la justificación
 procedimental, términos y condiciones de la contratación, ni del
 cumplimiento de los requisitos de la Ley de Adquisiciones, Arrendamientos
 y Servicios del Sector Público y sus disposiciones, así como de las
 disposiciones y las demás circunstancias que determinen procedente
 la presente inscripción, en el presente.

Los aspectos jurídicos del presente documento han sido validados por la
 titular de la Dirección Jurídica, en cumplimiento a lo dispuesto en el artículo 25
 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público,
 en el sistema electrónico de validación de la Dirección de Contratos y
 Compras de la Coordinación de Legislación y Consulta de la Unidad de Adquisiciones,
 en el presente. En consecuencia, el presente documento, en su totalidad, se
 encuentra registrado en el sistema de validación de la Dirección de Contratos y
 Compras de la Coordinación de Legislación y Consulta de la Unidad de Adquisiciones
 bajo el número 019E18222/Adquisiciones





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

CONTRATO
 NÚMERO
 019E18222-002

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 concurren 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 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.

Dirección Jurídica
 Unidad de Asesoría Consultiva y
 Coordinación de Legislación y Consulta

La validación jurídica se efectúa sin perjuicio sobre la justificación, prescripción, términos y condiciones de la contratación, ni del cumplimiento de los requisitos de la convocatoria, ni de la promoción a la licitación, ni de la procedencia de la solicitud de adjudicación económica y las demás circunstancias que determinan procedencia de la contratación, ni de la validez de la oferta.

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 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y se basa en el dictamen elaborado por la División de Dictamen Jurídico de Contratos y Compras de la Coordinación de Adquisición y Consulta de la Unidad de Asesoría Consultiva y Coordinación de Legislación y Consulta, en cumplimiento de lo dispuesto en el artículo 75 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, bajo el número de archivo: 019E18222/019E18222.



GOBIERNO DE MÉXICO



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

CONTRATO
 NÚMERO
 019E18222-002

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

Dirección General de
 Adquisiciones, Arrendamientos y
 Servicios del Sector Público
 Unidad de Adquisiciones, Arrendamientos y
 Servicios del Sector Público
 Coordinación de Adquisición de Bienes y
 Contratación de Servicios

GOBIERNO DE
 MÉXICO

La validación jurídica se efectuó sin aplazarse sobre la justificación, el presupuesto, el contrato, el procedimiento de mercado, el procedimiento de la contratación de mercado correspondiente, ni se pronunció sobre la procedencia y/o viabilidad de los aspectos técnicos, económicos, financieros, jurídicos, administrativos, de distribución, procedencia, las áreas específicas, Métrica y/o contractuales.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en el momento a lo dispuesto en el artículo 25 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en base en el dictamen elaborado por la División de Dictamen Jurídico de Contratos y Bienes, en el momento de la emisión de la resolución de adjudicación, de conformidad con el artículo 25 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y de Atención a Organizaciones Facilitadoras. En consecuencia, se registró bajo el número: 04080302/000/2016005



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

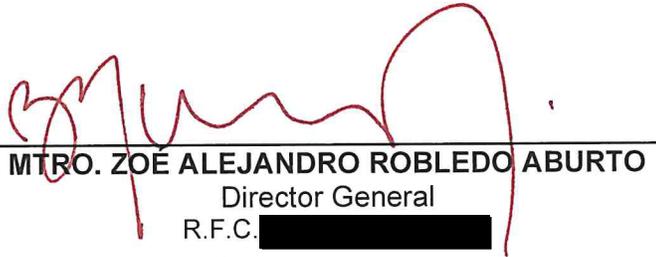
CONTRATO
 NÚMERO
 019E18222-002

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

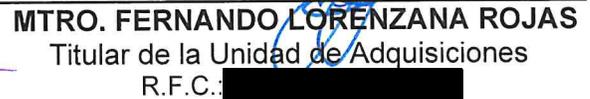

 MTRO. ZOÉ ALEJANDRO ROBLEDO ABURTO
 Director General
 R.F.C. [REDACTED]

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

GOBIERNO DE MÉXICO
 IMSS
 Dirección Jurídica
 Unidad de Asesoría Consultiva y Coordinación de Legislación y Consulta
 La validación jurídica se efectuó en principio sobre la identificación, términos y condiciones de la contratación, el procedimiento, los requisitos, la investigación y el resultado de la misma, así como la capacidad de los sujetos, sus antecedentes económicos y las demás circunstancias que determinaron procederes las bases requeridas, todas y por contrato.

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 PLANEACIÓN Y CONTRATOS

CONTRATO
 NÚMERO
 019E18222-002

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

ADMINISTRADOR DEL CONTRATO

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

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

POR "EL PROVEEDOR"
 CONSULTING ALL SERVICE IN TELECOM
 AND MEDICE,
 S. DE R.L. DE C.V.
 R.F.C.: CAS1211066S3
 (Participante A)

[Signature]
 C. JULIO CRUZ GÓMEZ
 Representante Legal

SECURE LABS, S.A. DE C.V.
 R.F.C.: SLA2001239H9
 (Participante B)

[Signature]
 C. ALBERTO VARGAS MAGAÑA
 Representante Legal

[Signature]
 C. FRANCISCO OVALLE FELIX
 Representante Legal

DIVISIÓN DE CONTRATOS
 NIVEL CENTRAL

Página 30

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".

Dirección Jurídica
 de Administración y Contratos
 de la Coordinación de Adquisición de Bienes y
 Contratación de Servicios

La validación jurídica se efectuó de acuerdo al precepto que establece el artículo 75 del Reglamento Interior del Instituto Mexicano del Seguro Social, en el que se dispone que la validación jurídica se efectuará sobre la procedencia y/o aptitud de los aspectos técnicos, económicos y financieros que determinan el procedimiento, así como sobre la legalidad de los actos administrativos, de conformidad con el artículo 268 A de la Ley del Seguro Social.

Los aspectos jurídicos del presente documento fueron validados por la persona titular de la Dirección Jurídica, en cumplimiento de lo dispuesto en el artículo 75 del Reglamento Interior del Instituto Mexicano del Seguro Social, en el que se dispone que la validación jurídica se efectuará sobre la procedencia y/o aptitud de los aspectos técnicos, económicos y financieros que determinan el procedimiento, así como sobre la legalidad de los actos administrativos, de conformidad con el artículo 268 A de la Ley del Seguro Social.



GOBIERNO DE MÉXICO

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 PLANEACIÓN Y CONTRATOS

CONTRATO
 NÚMERO
 019E18222-002

**BOHMER STRATEGISTS,
 S. DE R.L. DE C.V.**
 R.F.C.: BST2103235Z1
 (Participante C)

**C. ISIDORO GUILLERMO HERNÁNDEZ
 ZAGACETA**
 Representante Legal

RRSR/HRJ/LBGF/CMBS

Dirección Jurídica
 Unidad de Asesoría y
 de Asesoría a Organos Fiscalizadores
 de la Coordinación de Adquisición y Contratos

La validación jurídica se efectuó en pro de la justificación,
 procedimiento, términos y condiciones de la contratación, ni del
 procedimiento de adquisición de bienes y servicios, ni de la
 promoción sobre la procedencia y/o viabilidad de los aspectos técnicos,
 económicos, financieros, administrativos, de distribución presupuestal
 ni de las áreas requeridas, técnicas y/o contractuales.

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
 del Reglamento de la Ley Orgánica de la Administración Pública Federal, en
 base en el dictamen elaborado por la División de Dictamen Jurídico de Contratos y
 Compras de la Coordinación de Adquisición y Contratos, en la ciudad de México,
 a los días veintidós del mes de febrero del año dos mil diecinueve, en el
 expediente número BST2103235Z1/002/2019.



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

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 PLANEACIÓN Y CONTRATOS

**CONTRATO
NÚMERO
019E18222-002**

ANEXO 1 (UNO)

**“DICTAMEN DE DISPONIBILIDAD PRESUPUESTAL PREVIO Y
ACUERDO DEL H. CONSEJO TÉCNICO”**

**ANEXOS
DIVISIÓN DE CONTRATOS**

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

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: 0000439260-2022

Dictamen de Inversión
 Dictamen de Gasto

Dependencia Solicitante: 09 Distrito Federal Nivel Central
 099001 Oficinas Centrales
 580000 Coord de Servi Administr

Concepto: OF. 1554 RECIBIDO EL 05/10/2022 "SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA 2022-2024 PARTIDA 2"

Fecha Elaboración: 06/10/2022

Total Comprometido (en pesos): \$ 8,107,394.08
 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	4,053.7	4,053.7	
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	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 8º, 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-Millennium, 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

DÍA	MES	AÑO

DICTAMINADO DEFINITIVO

DICTAMEN DEFINITIVO

CONTRATO No. _____

IMPORTE DEFINITIVO (EN PESOS): \$ _____ .00

Clave: 6170-009-001

SIN TEXTO

Of N°09/9001/030000/2076

Ciudad de México, 27 de octubre de 2021.

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.

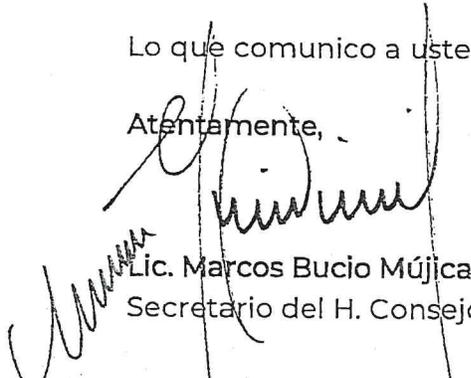
ANEXOS
DIVISIÓN DE CONTRATOS

H. Consejo Técnico

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 Andoníe. 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 Heraldéz 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



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

CONTRATO
NÚMERO
019E18222-002

ANEXO 2 (DOS)

“ANEXO TÉCNICO y TÉRMINOS Y CONDICIONES”

**ANEXOS
DIVISIÓN DE CONTRATOS**

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

SIN TEXTO



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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,





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 funcionalidades 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 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 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.



GOBIERNO DE
MÉXICO



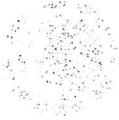
DIRECCIÓN DE ADMINISTRACIÓN
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022



Ricardo
2022 Flores
Año de
Magón

GOBIERNO DE LA FEDERACIÓN MEXICANA



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 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.

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)

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, análisis de ciberamenazas avanzadas, auditoría 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.





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Partida 2

1. Análisis de Vulnerabilidades Estático

El instituto requiere la continuidad de servicios de análisis de vulnerabilidades estáticos (aseguramiento de aplicaciones) 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 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 vulnerabilidades 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 dispositivos 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 dispositivos 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 dispositivos 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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.





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 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, así 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 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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

todos los dispositivos, así como garantizar que la bitácora de 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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.





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 dispositivos 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 dispositivos 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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*



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 dispositivos 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 inglés).
- 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 previsible, 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 genere 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 electrónico



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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).



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 coleccionar 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 pérdida 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.





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 inglés).
- 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 contraseñas 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 reporte y auditoría
- Capacidades de monitoreo y diagnóstico de problemas
- Administración de mensajes de eventos (logs) exportables.

6.2.7. Servicio de Antivirus



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 solicite, 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.





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 riesgosLa 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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:



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 auditorías.
 - 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:



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 trainees. 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 cumplimiento el *software* evaluado, las cuales podrán ser:
 - Al inicio del desarrollo de una aplicativo.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 dominan 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 Operation 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 de seguridad.
- Notificaciones y alertas personalizadas, en caso de desviaciones, anomalías 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 lo estipulado en los acuerdos de niveles de servicio



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 currículum 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 inglés) 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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

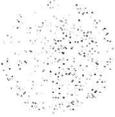
El proveedor del servicio de SASI 2022-2024, será responsable de llevar a cabo la implementación de los servicios solicitados conforme a los plazos descritos en el presente documento, lo cual incluye las renovaciones o migraciones de tecnología que el cumplimiento de SASI 2022-2024, implique para la 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 currículum 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 currículum vitae de todo el personal que participe en el servicio, se acreditará 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 demostrar	Función	Número de recursos
Administrador del Centro de Operaciones de Seguridad (SOC)	Se deberá presentar alguna las siguientes certificaciones vigentes: CISM (Certified Information Security Manager) CISSP (Certified Information Systems Security Professional) 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: PMP (Project Manager Professional) Certificado por PMI ITIL v4 (Expert o Master) 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: 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

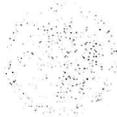


Licitación Pública Nacional Electrónica Número LA-050GYR019-EI82-2022

Perfil	Certificaciones a demostrar	Experiencia a demostrar	Función	Número de recursos
Arquitecto Especializado en Redes y Seguridad	Se deberá presentar alguna las siguientes certificaciones vigentes: CCNP (Cisco Certified Network Professional) CCIE Enterprise Infrastructure (Cisco Certified Internetwork Expert) 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 demostrar	Función	Número de recursos
Líder de proyecto	Se deberá presentar alguna las siguientes certificaciones vigentes: PMP (Project Manager Professional) Certificado por PMI ITIL v4 (Expert o Master) 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: 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Perfil	Certificaciones a demostrar	Experiencia a demostrar	Función	Número de recursos
Consultor de Penetración	Se deberá presentar alguna las siguientes certificaciones vigentes: GPEN (GIAC Certified Penetration Tester) 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 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: EnCE (EnCase Certified Examiner) 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. 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 (<i>Operational Level Agreement, OLA</i>)	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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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

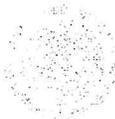




Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	<ul style="list-style-type: none"> Requerimientos Cambios Configuraciones Incidentes Problemas 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: <ul style="list-style-type: none"> Requerimientos Cambios Configuraciones Incidentes Problemas 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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

	Documento Compromiso de suscripción del acuerdo de niveles operacional (<i>Operational Level Agreement, OLA</i>)	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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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:



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Partida 1

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Seguridad – Continuidad Operativa	Reportes Técnicos de los activos de infraestructura que contemplen: <ul style="list-style-type: none"> • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • 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: <ul style="list-style-type: none"> • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • 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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 <i>software</i> 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
Servicios de Análisis Forense	Reporte que integre el calendario de actualizaciones de	Trimestral	5 días hábiles posteriores al

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	versionamiento en <i>software</i> 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 funcionarios 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 Auditoría" 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:



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 "Trojanos". 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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, así 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 periodo de transferencia de servicios al nuevo proveedor.

Dicho periodo 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.

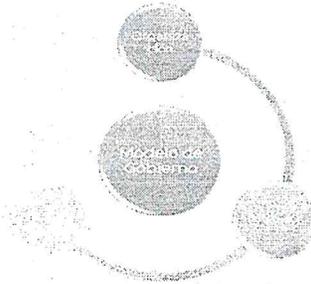
El Modelo de Gobierno comprende los principales aspectos a considerar para asegurar y controlar la operación del proyecto.

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 líderes del proyecto, con apoyo por parte del proveedor del servicio (SOC), garanticen los niveles de servicios establecidos para la operación.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022



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" 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".





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 inglés) 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.

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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.





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

4. Servicios de Protección contra Denegación (DDoS)

Table with 3 columns: Service, Tipo 1, Tipo 2. Rows include Desempeño, Conexiones simultaneas por seg., Conexiones nuevas por seg., and Interfaces 10GbE.

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:

- List of technical specifications including: Incluir un sistema operativo propietario del fabricante, El licitante deberá considerar en su propuesta que la cantidad de tráfico máximo a inspeccionar por los equipos y un ancho de banda de los enlaces de internet que estarán recibiendo los equipos, Deberá garantizar el paso transaccional de datos legítimos, Detección del tráfico basado en el lenguaje TCPDUMP, Deberá tener la capacidad de advertir anticipadamente algún posible ataque, 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, Detección de ataques basado en la línea de base contra los recursos definidos, 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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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.





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 explícito 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 reporte centralizado incluyendo control de acceso discrecional, control de versiones, auditoría 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).
- Auditoría 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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), phishing 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).



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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.
- Auditoría 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).



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 ICASA 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
 - XHTML
 - HTML5
 - XML
 - JSON
 - AJAX
 - FLASH

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

El licitante deberá considerar en su propuesta que la característica de conexiones simultáneas 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 soportar 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 tuneo 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.





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 explícito 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).



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 accedido (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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 inglés) 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 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)
- 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 movimientos 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 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).
 - 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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.





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

14. Servicios de Prevención de Pérdida 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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).



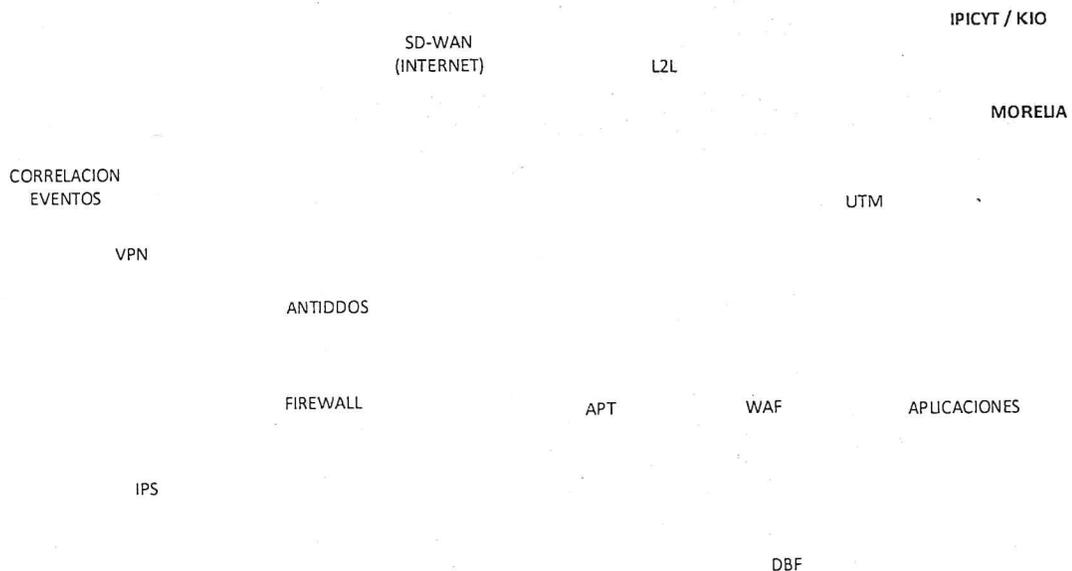


Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- De las propuestas de solución, podrán proponer arreglos tipo cluster.

DIAGRAMA 01. PROPUESTA MÍNIMA ESPERADA DE LAS SOLUCIONES

RED INTERNA

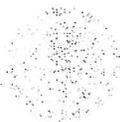


16. Especificaciones físicas y estándares de conexión para los insumos que conforman los Servicios Administrados de Seguridad Informática 2022-2024

- 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.





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 centros 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 (Patch 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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	F11K5FTE20000010
	CENATI MONTERREY	Fortinet	FDD-1500F	F11K5FTE20000039



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



GOBIERNO DE
MÉXICO



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

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Tipo 3	CENATI MONTERREY	Fortinet	FG-600E- BDL-950-12	FG6H0ETB21901099
Tipo 4	CENATI MÉXICO	Fortinet	FG-1800F- BDL-950-12	FG180FTK20901163



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

18	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 3) - Renovación	de Servicio	1	1
19	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 4) - Renovación	de Servicio	1	1





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 proteja 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,



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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.

- Cuento 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.
- Cuento 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

- Certificado ISO/IEC27001:2013
- Certificado 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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
<p><u>Procedimientos de Operación del servicio</u></p> <ul style="list-style-type: none"> • Servicios de Borrado Seguro de Información • Servicio de Gestión de Dominios • Servicio de Certificados Digitales SSL • Servicios de Ciberinteligencia • Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos móviles • Servicios de Antivirus • Servicios de Prevención de Pérdida 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
<p>Metodología de implementación de los servicios.</p> <ul style="list-style-type: none"> • 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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Información (SGSI) <ul style="list-style-type: none"> 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> <ul style="list-style-type: none"> Servicio de Análisis de Vulnerabilidades Estático Servicio de Análisis de Vulnerabilidades Dinámico Servicios de Análisis Forense 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

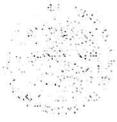
DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Procesos de operación implementados: <ul style="list-style-type: none"> Requerimientos Cambios Configuraciones Incidentes Problemas Monitoreo 	15 días naturales posteriores a la emisión del fallo	2% por cada 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
<u>Procedimiento de operación de la Mesa de Servicios:</u> <ul style="list-style-type: none"> Requerimientos Cambios Configuraciones Incidentes Problemas 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



Licitación Pública Nacional Electrónica Número LA-050CYR019-E182-2022

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.

Disponibilidad del Servicio = [(Tiempo_Total - (Tiempo_Indisponible - Tiempo_Instituto)) / Tiempo_Total] X 100

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:

Table with 2 columns: Disponibilidad Servicio, % Disponibilidad





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 Crítica: 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.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 periodos 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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 crítica	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 crítica	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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 envío 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 crítica	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 crítica	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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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, entendiéndose 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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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:





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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: <ul style="list-style-type: none"> • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • 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

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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: <ul style="list-style-type: none"> • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Falla • Actividad Sospechosa • 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 de los Sistemas de Gestión	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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Servicio 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 (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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
herramientas tecnológicas utilizadas para el proceso de análisis				
<p>Servicios de Pruebas de Penetración:</p> <p>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</p>	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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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				
<u>Servicios de Análisis Forense:</u> Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectados 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050CYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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	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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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.

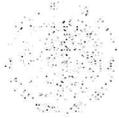
11. Condiciones de Pago

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Documento Compromiso de suscripción del acuerdo de niveles operacional (<i>Operational Level Agreement, OLA</i>)	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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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: <ul style="list-style-type: none"> • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • 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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Procedimiento de operación de la Mesa de Servicios: <ul style="list-style-type: none"> • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • 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 (<i>Operational Level Agreement, OLA</i>)	Única Vez	15 días naturales posteriores a la emisión del fallo
	Matriz de Escalación	Única Vez	





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

			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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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



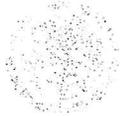


Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 detectados 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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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: <ul style="list-style-type: none"> • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • 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: <ul style="list-style-type: none"> • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • 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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 funcionarios 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 Auditoría" 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 ponderación establecida en la matriz de evaluación correspondiente.

18. Funcionarios públicos de la DIDT participantes en el proceso de contratación



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 Osmary 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



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

24. Otorgamiento de anticipo

No aplica





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

CONTRATO
NÚMERO
019E18222-002

ANEXO 3 (TRES)

“PROPUESTA TÉCNICA Y ECONÓMICA DE “EL PROVEEDOR” Y ACTA DE FALLO”

**ANEXOS
DIVISIÓN DE CONTRATOS**

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

SIN TEXTO



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

PROPUESTA TÉCNICA ANEXO 1 Y ANEXO 2

Para la Contratación de los:
"Servicios Administrados de Seguridad Informática (SASI) 2022-2024"

Licitación Pública Nacional Electrónica
Núm. LA-050GYR019-E182-2022

Partida 2

RFC de los integrantes del Consorcio:
Participante A: CAS1211066S3
Participante B: SLA2070239HS
Participante C: B5T240395Z1

ANEXOS
DIVISIÓN DE CONTRATOS



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 1.- Anexo Técnico

1. Objetivo del Documento

EL CONSORCIO, presenta en este documento su propuesta técnica (PARTIDA 2) que contiene los servicios conforme a los requerimientos y especificaciones técnicas y de calidad que solicita el Instituto.

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

- Asegurará y protegerá la información Institucional.
- Garantizará 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.
- Fortalecerá 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.
- Contará 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.
- Contará 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.
- Contará 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



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

forense y de procesos de seguridad, así como con otros servicios especializados en materia de seguridad y tecnologías de la información.

- Contará 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:

- Contará 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.
- Proporcionará 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.
- Contará 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.
- Proporcionará 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.



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Garantizará 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 funcionalidades en materia de seguridad o para aquellos que requieran de una sustitución (por falla) o un reajuste. Por lo tanto, el consorcio conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.; XXX, XXX y XXX (en lo sucesivo EL CONSORCIO), conoce y acepta que el IMSS está en continua evolución tecnológica, por lo que se apegará 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 CONSORCIO, conoce y acepta que el IMSS está en continua evolución tecnológica, por lo que se apegará a ella en todo momento.

EL CONSORCIO, 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, EL CONSORCIO, considerará lo establecido en el apartado de "Penas Convencionales y Deduciones".

EL CONSORCIO, 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.

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.



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

5. Requerimientos del servicio

Los Servicios requeridos y que serán parte de la solución propuesta por EL CONSORCIO, se desagregan por partida, mismos que incluyen al menos lo siguiente:

Partida 2

1. Análisis de Vulnerabilidades Estático

EL CONSORCIO, proveerá al instituto la continuidad de servicios de análisis de vulnerabilidades estáticos (aseguramiento de aplicaciones) 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 el desarrollo de aplicaciones en sus diferentes etapas de construcción.

2. Análisis de Vulnerabilidades Dinámico

EL CONSORCIO, proveerá al instituto la continuidad de servicios de análisis de vulnerabilidades 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 CONSORCIO, proveerá al Instituto 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 CONSORCIO, proveerá al Instituto 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.

EL CONSORCIO, entiende que proveerá los servicios objeto de esta contratación a la partida 2, aquél 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, EL CONSORCIO, participar únicamente en la partida 2, lo anterior para evitar conflicto de interés técnico en detrimento del IMSS.

En este sentido, EL CONSORCIO, toma conocimiento de 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.



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

6. Requerimientos del Servicio - Especificaciones Técnicas

Partida 1.: NO PARTICIPA EL CONSORCIO

6.1. Servicios de Seguridad – Continuidad Operativa

6.1.1. Servicios de Firewall

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6.1.2. Servicios de Prevención de Intrusos (IPS)

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6.1.4. Servicios de Redes Privadas Virtuales (VPN)

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6.1.5. Servicios de Filtrado de Contenido Web

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6.1.9. Servicios de Gestión Unificada de Amenazas (UTM)

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GR019-E182-2022

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6.1.10. Servicio de Correlación de Eventos

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6.2. Servicios de Seguridad – verificación y calidad

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6.2.1. Servicios de Borrado Seguro de Información

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6.2.2. Servicio de Gestión de Dominios

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6.2.3. Servicio de Certificados Digitales SSL

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6.2.4. Servicios de Ciberinteligencia (Ciberseguridad)

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6.2.7. Servicio de Antivirus

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6.2.8. Servicios de Prevención de Pérdida de Información

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

RFC de los Interconexos del Consorcio:
Participante A: CAS121106653
Participante B: SLA2001259MS
Participante C: BST210525Z1



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

Partida 2

6.2.11. Servicios de Análisis de Vulnerabilidades Dinámico

Descripción del servicio.

EL CONSORCIO, proveerá al Instituto 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 CONSORCIO, cumplirá con las siguientes especificaciones funcionales mínimas.

- Integrará 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.
- Dará 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 permitirá continuar con los servicios y activos de infraestructura que correspondan.
- Garantizará 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.
- Identificará 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

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Sensitive Data Exposure
 - Security Misconfiguration
 - Broken Authentication and Session Management
- Elaborará 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.
 - Integrará un proceso y/o procedimiento para la continuidad de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada.
 - EL CONSORCIO, como proveedor de servicios integrará 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.

EL CONSORCIO Aplicará diferentes herramientas según las características de la infraestructura tecnológica, objetivos y alcances de las pruebas, las cuales tienen entre sus funciones servir como Scanners, sniffer, web exploits, OS exploits y DB exploits. Los usos y capas donde aplicamos las diferentes herramientas son:

					
Escáner de seguridad de aplicaciones web de código abierto. Permite al usuario manipular todo el tráfico que pasa a través de él, incluido el tráfico mediante https	Detección y enumeración de sistema operativo y aplicaciones en base a la información que se pueda obtener del servicio detectado	Análisis de vulnerabilidades con mapeo de exploits. Detección y enumeración de sistema operativo y aplicaciones en base a servicios detectados	Framework para realizar las pruebas de explotación de servicios y vulnerabilidades identificadas en sistemas operativos y aplicativos WEB	Herramienta especializada en análisis de vulnerabilidades y pruebas de penetración en aplicaciones web	Escáner de seguridad de aplicaciones web de código abierto. Permite a los usuarios manipular todo el tráfico que pasa a través de él, incluido el tráfico mediante https
Aplicativos webs	Aplicativos webs Bases de datos Infraestructura Red	Aplicativos webs Bases de datos Infraestructura Red	Aplicativos webs Bases de datos Infraestructura Red	Aplicativos webs Bases de datos Infraestructura	Aplicativos webs
					
Gophish. Herramienta especializada para realizar campañas de phishing	Motor de búsqueda que proporciona información sobre los activos que se han conectado a la red	Nikto. Escáner de servidores web de código abierto que realiza pruebas exhaustivas contra servidores web	Análisis de vulnerabilidades con mapeo de exploits	SQLmap. Herramienta de código abierto que automatiza el proceso de detección de exploits SQL	Analizador de tráfico web gráfico que facilita la obtención de información de los paquetes enviados a través de la red
Usuarios	Bases de datos Infraestructura Red	Aplicativos webs	Aplicativos webs Bases de datos Infraestructura Red	Aplicativos webs Bases de datos	Red Físico

6.2.12. Servicios de Análisis de Vulnerabilidades Estático

Descripción del servicio.

EL CONSORCIO, proveerá al Instituto identificar el nivel inicial de madurez de las prácticas de seguridad en el software con las que cuenta el Instituto, por lo que EL CONSORCIO, cumplirá con las siguientes especificaciones funcionales mínimas.



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

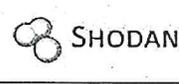
- Implementará una solución tecnológica que permita realizar pruebas dinámicas y estáticas de una manera centralizada y con soporte al menos a los siguientes lenguajes de programación: HTML, Java, .Net, C#, PHP.
- Integrará el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- Garantizará 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.
- Integrará un proceso de evaluación de las prácticas existentes de seguridad de software en el Instituto.
- Construirá un programa de evaluación de seguridad de software con iteraciones definidas en conjunto con el Instituto.
- Actualizará y creará procesos en las diferentes etapas del ciclo de vida de desarrollo de software para asegurar el mismo.
- Ayudará en el cumplimiento del software basado en estándares y/o marcos normativos previamente definidos en conjunto con el Instituto.
- Identificará el nivel inicial de madurez de las prácticas de seguridad en el software con las que cuenta el Instituto.
- Identificará y entenderá 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 serán incluidas en el proceso.
- Integrará 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.
- Operará el modelo de madurez establecido, pudiendo certificar en 3 diferentes etapas el nivel de cumplimiento 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.
- Preservará la integridad y confidencialidad de la información recibida durante la ejecución de las pruebas dinámicas y/o estáticas correspondientes (cadena de custodia).

RFC de los integrantes del Consorcio:
Participante A: C05421106553
Participante B: SLA2001208919
Participante C: B57210323521

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. Y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Elaborará 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.

EL CONSORCIO Aplicará diferentes herramientas según las características de la infraestructura tecnológica, objetivos y alcances de las pruebas, las cuales tienen entre sus funciones servir como Scanners, sniffer, web exploits, OS exploits y DB exploits. Los usos y capas donde aplicamos las diferentes herramientas son:

 OWASP ZAP	 NMAP	 nexpose	 metasploit	 BURP SUITE PROFESSIONAL	 VEGA
Escáner de seguridad de aplicaciones web de código abierto. Permite al usuario manipular todo el tráfico que pasa a través de él, incluido el tráfico mediante https	Detección y enumeración de sistema operativo y aplicaciones en base a la información que se pueda obtener del servicio detectado	Análisis de vulnerabilidades con mapeo de exploits. Detección y enumeración de sistema operativo y aplicaciones en base a servicios detectados	Framework para realizar las pruebas de explotación de servicios y vulnerabilidades identificadas en sistemas operativos y aplicativos WEB	Herramienta especializada en análisis de vulnerabilidades y pruebas de penetración en aplicaciones web	Escáner de seguridad de aplicaciones web de código abierto. Permite a los usuarios manipular todo el tráfico que pasa a través de él, incluido el tráfico mediante https
Aplicativos webs	Aplicativos webs Bases de datos Infraestructura Red	Aplicativos webs Bases de datos Infraestructura Red	Aplicativos webs Bases de datos Infraestructura Red	Aplicativos webs Bases de datos Infraestructura	Aplicativos webs
 Gophish. Herramienta especializada para realizar campañas de phishing	 SHODAN	 Nikto. Escáner de servidores web de código abierto que realiza pruebas exhaustivas contra servidores web	 Nessus vulnerability scanner	 SQLmap. Herramienta de código abierto que automatiza el proceso de detección de exploits SQL	 WIRESHARK
Usuarios	Bases de datos Infraestructura Red	Aplicativos webs	Aplicativos webs Bases de datos Infraestructura Red	Aplicativos webs Bases de datos	Red Físico

6.2.13. Servicios de Pruebas de Penetración

Descripción del servicio.

EL CONSORCIO, proveerá al Instituto 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 CONSORCIO, cumplirá con las siguientes especificaciones funcionales mínimas.

- Integrará 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.
- Dará seguimiento a los servicios o activos de información que serán 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

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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

- Realizará un reporte ejecutivo y técnico, por cada requerimiento atendido, en el que se describirán 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.

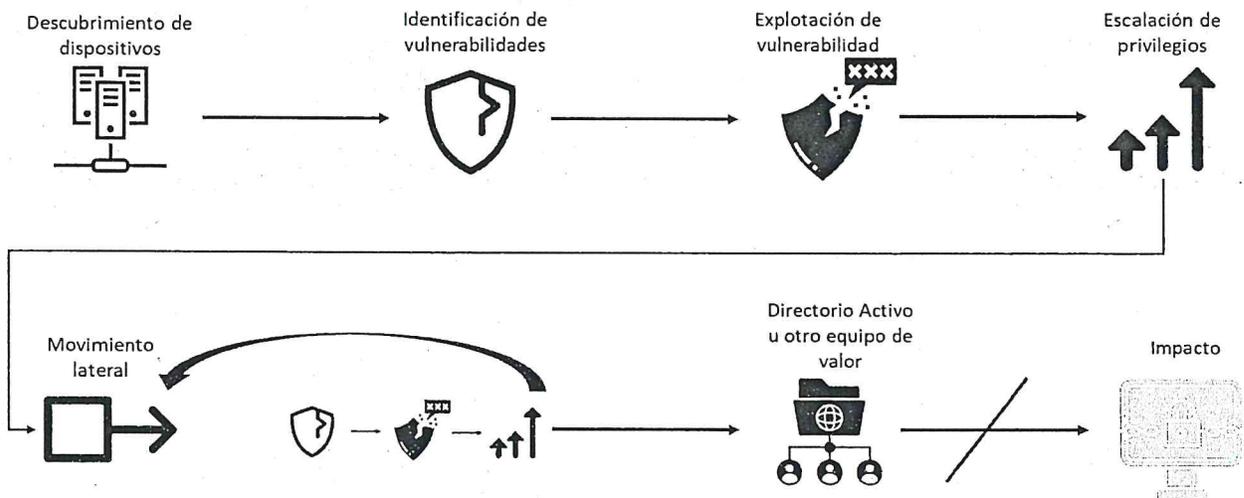
- Integrará un proceso y/o procedimiento para la continuidad de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada.

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- EL CONSORCIO, como proveedor de servicios integrará 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.

EL CONSORCIO usará técnicas equivalentes a las de los atacantes avanzados, para de manera secuencial alcanzar el máximo nivel de compromiso/acceso en el menor tiempo posible. Por lo anterior, se identificarán vulnerabilidades potenciales, y se utilizarán aquellas que permitan alcanzar el máximo nivel de acceso; estas y el resto se reportarán para su remediación.

El modelo de ejecución se describe en el siguiente diagrama:



6.2.14. Servicios de Análisis Forense

Descripción del servicio.

EL CONSORCIO, proveerá al Instituto 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 CONSORCIO, como proveedor de servicios cumplirá con las siguientes especificaciones funcionales mínimas.

- Integrará 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.
- Continuará con la definición del objetivo parámetros y cuestionario que resulten de interés para la investigación solicitada.
- Dará continuidad y seguimiento a los casos solicitados, así como, el registro de los indicadores correspondientes.



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

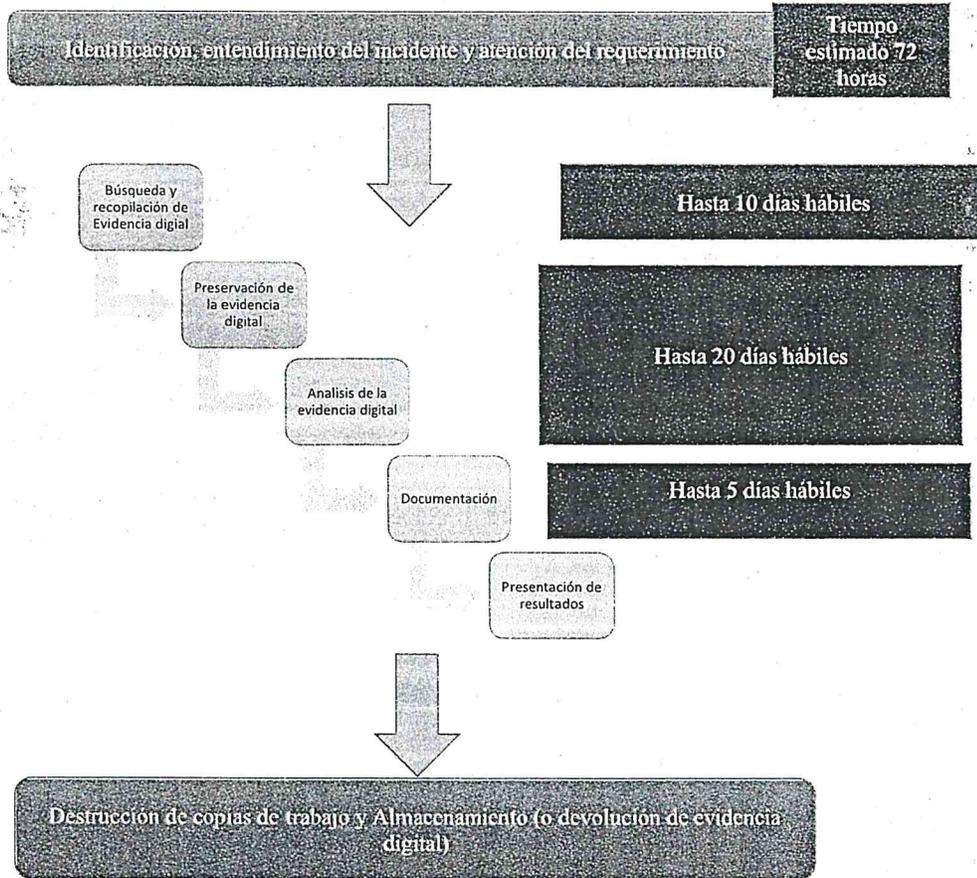
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Preservará la integridad de la información recibida durante la ejecución del proceso de análisis forense (cadena de custodia).
- Participará en entrevistas con los principales involucrados con la finalidad de obtener el contexto necesario en las investigaciones digitales que deban realizarse.
- Obtendrá información de fuentes públicas en la red en caso de que estas pudieran llegar a ser relevantes para la investigación realizada.
- Realizará 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.
- Llevará a cabo un proceso de recuperación de información que haya sido borrada previamente.
- Dará 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.
- Elaborará 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 dominan el lenguaje técnico.

METODOLOGÍA DE SERVICIOS DE FORENSE DIGITAL.

La metodología que sigue EL CONSORCIO para la entrega de servicios relacionados con Forense Digital consiste de la aplicación de las siguientes etapas:

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022



Magnet AXIOM Cyber

Una solución de análisis forense digital diseñada para satisfacer las necesidades de las organizaciones que realizan adquisiciones remotas, así como recopilar y analizar evidencia de servicios de comunicación y almacenamiento en la nube, computadoras y dispositivos móviles.

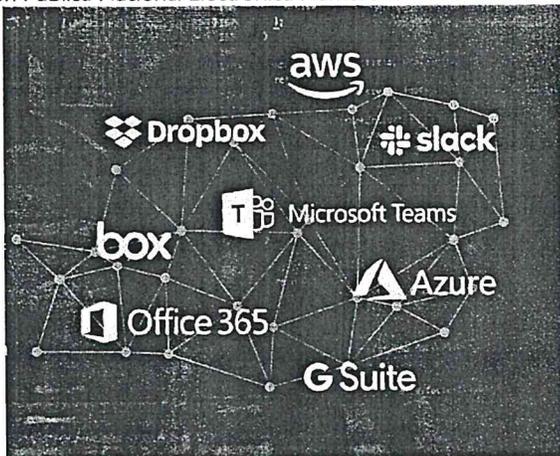
Cloud

Los servicios en la nube han cambiado la forma en que los empleados comunicar, compartir y almacenar información. Aproveche las credenciales de administrador o usuario para acceder a los registros de auditoría y examinar las cuentas en la nube de los empleados sin avisarles sobre una investigación en curso.

AXIOM Cyber adquiere y analiza datos de empresas servicios de almacenamiento en la nube como AWS S3, EC2 y Azure, además a otras fuentes en la nube, incluidas Office 365, G Suite, Box, Dropbox, Slack y iCloud

RFC de las Insurgencias del Consorcio:
 Participante A: CA56121106653
 Participante C: SLA2032239118
 Participante G: B5721322521

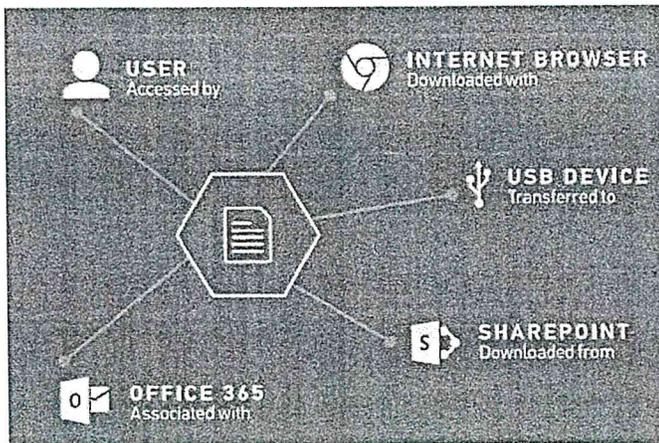
Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022



Computer

AXIOM Cyber proporciona la colección más completa y poderosa de herramientas de recuperación, búsqueda, análisis y generación de informes para Mac y PC.

Funciones analíticas potentes e intuitivas en AXIOM Cyber como Timeline, Connections y Magnet.AI le permiten centrarse en los datos más relevantes, lo que le permite trabajar su presente su caso de forma más rápida y sencilla a los departamentos de Recursos Humanos, Legal y otras partes interesadas.



MOBILE

AXIOM Cyber es una parte esencial para iOS e investigaciones de Android. Técnicas integrales de análisis y búsqueda encontrar más artefactos como el historial del navegador, chats, correos electrónicos y documentos. Visualice y presente pruebas fácilmente mostrando correos electrónicos y chats en su formato original que a menudo se necesitan para recursos humanos investigaciones como mala conducta de los empleados o casos de acoso.

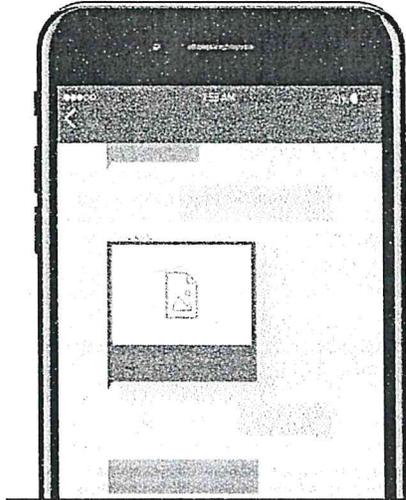
RFC de licitantes del consorcio:
 Participante A: C-06521106653
 Participante B: 9LA203232199
 Participante C: 831243023521



CALLIT

TELECOMUNICACIONES
Y SERVICIOS DE TELECOMUNICACIONES
DEL ESTADO DE QUERÉTARO
S.A. DE C.V.
CALLE DEL COMERCIO 1000
QUERÉTARO, QUERÉTARO, QUERÉTARO

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022



Herramientas de Forense

Forensic ComboDock, model FCDv6 - Write-blocked or read/write Access



Drive eRazer Ultra



Ditto Field Kit K-DX

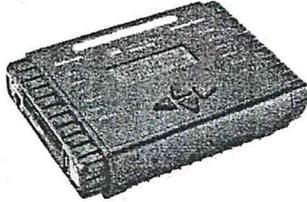


RFC de los integrantes del Consorcio:
Participante A: CAS1211066S3
Participante B: SLA2001239H9
Participante C: R5721032573



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Ditto DX Forensic FieldStation



6.3. Servicios del Centro de Operaciones de Seguridad (SOC)

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6.5. Condiciones para la implementación de los servicios

EL CONSORCIO, como proveedor de servicios SASI 2022-2024 (PARTIDA 2), 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 CONSORCIO, como proveedor de servicios SASI 2022-2024 (PARTIDA 2), 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 (PARTIDA 2). 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 CONSORCIO, a la red del Instituto, y será a cargo de EL CONSORCIO, en caso de resultar adjudicado.

Para la instalación, configuración y habilitación de cada una de las soluciones de los servicios, EL CONSORCIO, como proveedor de servicios de SASI 2022-2024 (PARTIDA 2) 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), y el Instituto.

Es importante señalar que, EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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, EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), entenderá el control de cambios como

RFC de los integrantes del Consorcio:
Participante A: CAS121106653
Participante B: SLAZ0223919
Participante C: EST21032954

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 (PARTIDA 2), 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, quedará incluido en la propuesta de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2).
- **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 brindarán en los componentes habilitadores que EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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, EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), será el responsable de asignar personal con experiencia y expertos para conformar las mesas de trabajo. En caso de que el personal asignado sea retirado del servicio de



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SASI 2022-2024, será responsabilidad de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO están validadas por personal certificado y con experiencia.
- 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 con 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.



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

6.8. Perfil del Proveedor

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 el presente Anexo Técnico.

El personal de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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, integramos el currículum 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 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 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 currículum vitae de todo el personal que participará en el servicio de la PARTIDA 2, se acreditará 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.

EL CONSORCIO, acreditará al menos la licenciatura o ingeniería en informática, telecomunicaciones, computación o carrera a fin del personal propuesto, en los términos que establece la Ley Reglamentaria del Art. 5 Constitucional, la acreditación será con el título o cédula profesional y para el caso de estudios en el extranjero, estos estarán avalados por las instancias oficiales correspondientes, así como estar debidamente apostillados.

A continuación, se listan las credenciales y capacidades que cubren los recursos asignados al proyecto:

Partida 1

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

Partida 2

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Perfil	Certificaciones a demostrar	Experiencia a demostrar	Función	Número de recursos
Líder de proyecto	Se presenta alguna las siguientes certificaciones vigentes: PMP (Project Manager Professional) Certificado por PMI ITIL v4 (Expert o Master) 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 presenta la siguiente certificación vigente: 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
Consultor de Penetración	Se presenta alguna las siguientes certificaciones vigentes: GPN (GIAC Certified Penetration Tester) 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 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 presenta alguna las siguientes certificaciones vigentes: EnCE (EnCase Certified Examiner) 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. Tiene la capacidad de ejecutar investigaciones forenses en caso de ser necesario	Al menos 1

RFC de los integrantes del Consorcio:
Participante A: CAS121106653
Participante B: SLA200129H9
Participante C: EST1210303521

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), efectuará bajo la supervisión de los funcionarios designados por este último para tales efectos.

Partida 1

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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	Única Vez	15 días naturales posteriores a la emisión del fallo

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA20122819
 Participante C: G31740321523

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

	legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios		
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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), de manera enunciativa más no limitativa, generará entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

Partida 1.

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

Partida 2

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Reporte Técnico y Ejecutivo en formato electrónico (MS Word,	Evento	7 días hábiles posteriores a la solicitud

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades Dinámico	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 para el proceso de análisis		generada por parte del Instituto
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	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto

REC. de las Integridades del Consorcio:
 Participante A: CAS121106653
 Participante C: SLA201023918
 Participante B: B8721632374

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	hallazgos y que incluya 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 (código) 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

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA300123919
 Participante C: 95710382621

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

7.3. Entregables Periódicos

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), de manera enunciativa más no limitativa, generará entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

Partida 1

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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
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, serán entregados en formato electrónico (MS Word, MS Excel, PDF) conforme los periodos estipulados por el Instituto.

De igual manera, EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 funcionarios que sean designados por el primero mencionado.

RFC de los integrantes del Consorcio:
 Participante A: CA5121106653
 Participante B: SL3201123946
 Participante C: B57211323511



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

8. Niveles de servicio que se cumplirán (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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2).
- 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 a EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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".

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

10. Convenio de Confidencialidad y Resguardo de la Información

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), suscribirá el Convenio de Confidencialidad y Resguardo de Información correspondiente. En complemento, EL CONSORCIO considera al menos los siguientes mecanismos de control de acceso a la información del IMSS:

- Se establecerán controles de acceso y privilegios restringidos al personal de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del IMSS.
- EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), implantará y aceptará en todo momento el uso de controles que permitan establecer "Pistas de Auditoría" para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.
- Los empleados de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), con acceso a la información sensible del IMSS, firmarán acuerdos de confidencialidad con este.
- 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.
- EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), permitirá el acceso a información relacionada con el servicio prestado al IMSS para la realización de auditorías.
- EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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

No aplica

12. Normatividad Aplicable

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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. Las políticas aplicables se le darán a conocer durante las mesas de trabajo, sin embargo, se considerarán 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 EL CONSORCIO (partida 2).

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

13. Cumplimiento de Políticas

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), que estén involucrados en la prestación de los servicios, estarán protegidos con sistemas de detección de intrusos, control de infecciones virales, detección y eliminación de programas tipo "back door" o "Trojanos". Esta regla aplica tanto para los equipos de cómputo móviles (laptops, handheld, smartphones, tablet PC, etc.) como para los equipos de escritorio (desktop, desktside, 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2).

14. Finalización del Contrato

En el caso de terminación anticipada del contrato o a la finalización de la vigencia del mismo, EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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.

RFC de los integrantes del Consorcio:
Participante A: CAS121166632
Participante B: SLA300128119
Participante C: S8123032521



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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, EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), haya presentado previamente, y que el IMSS hubiera aprobado. No obstante, durante dicho periodo, EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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.

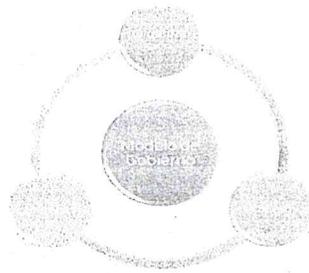
Dicho modelo establece la organización y los roles que participarán por parte del Instituto dentro del proyecto.

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 del proveedor del servicio (SOC), garanticen los niveles de servicios establecidos para la operación.

RFC de los integrantes del Consorcio:
Participante A: CAS121106653
Participante B: SAZ03123919
Participante C: 65721032524



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022



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" 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".

RFC de los integrantes del Consorcio:
- Participante A: CAS121106653
- Participante B: SUJ001239H9
- Participante C: RST123032371



CALLIT

SECRETARÍA DE ECONOMÍA
SUBSECRETARÍA DE ECONOMÍA
DIRECCIÓN GENERAL DE ECONOMÍA
DIRECCIÓN DE LICITACIONES
CALLE DE LOS RÍOS, S/N. P.O. BOX 358
MEXICO, D.F. C.P. 06300

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Apéndice "A"

Servicios Administrados de Seguridad Informática (SASI) 2022-2024

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

3. Servicio de Prevención de Intrusos (IPS)

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

4. Servicios de Protección contra Denegación (DDoS)

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

5. Redes Privadas Virtuales – VPN (C2S – S2S)

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

6. Filtrado de Contenido Web

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

7. Servicios de Filtrado de Contenido de Correo (Antispam)

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

8. Firewall Especializado en Servicios Web (WAF)

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

9. Servicios de Gestión Unificada de Amenazas (UTM)

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

10. Firewall Especializado en Base de Datos (DBF)

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

REC de los integrantes del Consorcio:
Participante: CASI12110666S
Participante: BOHMER STRATEGISTS
Participante: C: 3512-0182524

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

11. Servicio de Correlación de Eventos
NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

12. Servicio de Protección de Amenazas Persistentes Avanzadas (APT)
NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

13. Antivirus
NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

14. Servicios de Prevención de Pérdida de Información
NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

15. Generales para todas las soluciones
NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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 centros de datos para la alimentación eléctrica (contactos regulados), para el funcionamiento y operación del equipamiento propuesto por EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), considerará 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), instale la infraestructura de redes y seguridad en los centros de datos correspondientes. Para tal efecto EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), incluirá 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 contará con las facilidades para su instalación y se apegará al reglamento y políticas internas para la instalación dentro de cada Centro de Datos. Así también indicará 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 de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 considerará todo lo necesario con la finalidad de proveer lo necesario.

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Especificación para racks

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), cumplirá 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), cumplirá 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), suministrará los elementos para la interconectividad necesarios, por lo que: proporcionará e implementará 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), contemplará 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 se incluirán como parte de la propuesta de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), y serán sin costo extra para el IMSS. Asimismo, en el caso de incrementos en los servicios estarán 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, se incluirán como parte de la propuesta de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), y serán sin costo extra para el IMSS. Asimismo, en el caso de incrementos en los servicios estarán incluidos.

- Políticas de seguridad de acceso físico a externos

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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.

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Especificación y requerimientos de sistema de canalización.

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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, EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), realizará al menos un mantenimiento preventivo al año a toda la infraestructura que forme parte del contrato de SASI 2022-2024. Para lo cual integrará 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), incluirá un Plan de Mantenimiento Preventivo, el cual considera 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 se agrupará por tipo de equipo o infraestructura. Para cada caso, EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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.

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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), será responsable de realizar el mantenimiento correctivo para los servicios correspondientes de SASI 2021-2024, para lo cual, previamente integrará 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.

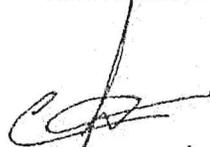
Como parte de las Mesas de Trabajo, EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), proporcionará la Matriz de Escalamiento con los nombres de contactos y responsables.

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), proporcionará un equipo provisional para mantener la operación. El tiempo para el reemplazo de equipos no excederá los 45 días naturales, durante los cuales EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), proporcionará un equipo provisional para mantener la operación.

Protesto lo necesario.

ATENTAMENTE



JULIO CRUZ GÓMEZ

APODERADO LEGAL DE CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.
Y REPRESENTANTE COMÚN DEL CONSORCIO CONFORMADO POR CONSULTING ALL SERVICE IN TELECOM
AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V.

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Apéndice "B"

Servicios Administrados de Seguridad Informática (SASI) 2022-2024

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

Apéndice "B-bis"

Servicios Administrados de Seguridad Informática (SASI) 2022-2024

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

1

Precisión 3.

Se anexa tabla que contiene los valores referenciales mínimos y máximos a considerar por la Partida 2 en el cuál EL CONSORCIO participa

PARTIDA 2			
49	Análisis de Vulnerabilidades Estático	160	400
50	Análisis de Vulnerabilidades Dinámico	320	800
51	Pruebas de Penetración	320	800
52	Análisis Forense	4	10



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 2.- Términos y Condiciones

1. Objetivo del documento

EL CONSORCIO, en caso de resultar adjudicado, se apegará a las necesidades y condiciones de entrega de los "Servicios Administrados de Seguridad Informática 2022-2024" (PARTIDA 2).

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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), se obliga a utilizarlas exclusivamente para cubrir los servicios requeridos.

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), presentará 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" (PARTIDA 2)

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.
- Cuenten 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.



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Cuenta 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.
- Cuenta 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.
- Cuenta 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

EL CONSORCIO, presenta las siguientes certificaciones, ambas vigentes y a su nombre siendo las siguientes:

- Certificado ISO/IEC27001:2013
- Certificado ISO/IEC20000-1:2018

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.

EL CONSORCIO, participa en Partida 2,

9. Garantías

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), no cumpla con los tiempos y plazos de entrega establecidos en los presentes Términos y Condiciones.



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Las modificaciones a las fianzas se formalizarán 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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.

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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.



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- 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 de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022.

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
			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

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

10.4 Servicios de Seguridad – Verificación/Calidad

Partida 1

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

Partida 2

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
<u>Procedimientos de Operación del servicio</u> <ul style="list-style-type: none"> Servicio de Análisis de Vulnerabilidades Estático Servicio de Análisis de Vulnerabilidades Dinámico Servicios de Análisis Forense 	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



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
<ul style="list-style-type: none"> Servicio de Pruebas de Penetración 			

10.5 Servicios del Centro de Operaciones de Seguridad (SOC)

Partida 1

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

10.6 Deducciones

Durante la vigencia del contrato, al presentarse 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), se aplicarán deductivas conforme lo siguiente rubros:

10.7 Disponibilidad

Partida 1

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

10.8 Tiempo de detección y solución de fallas

Partida 1

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

10.9 Tiempo de detección y mitigación de incidentes

Partida 1

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

10.10 Solicitudes de requerimientos y cambios



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Partida 1

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

10.11 Servicios de Seguridad – Continuidad Operativa

Partida 1

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

10.12 Servicios de Seguridad – Verificación/Calidad

Partida 1

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

Partida 2

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
<u>Servicio de Análisis de Vulnerabilidades Estático</u> 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	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



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CÓNCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
para el proceso de análisis				
<u>Servicio de Análisis de Vulnerabilidades Dinámico</u> 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 para el proceso de análisis	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
<u>Servicios de Pruebas de Penetración:</u> 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	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

RFC de los integrantes del Consorcio:
 Participante A: CAS121106634
 Participante B: SLA201123119
 Participante C: BST121032621

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
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				
<u>Servicios de Análisis Forense:</u> Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectados 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) NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2).

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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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-421231-145; 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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, presentando 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.

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

12. Entregables

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), de manera enunciativa más no limitativa, generará entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

Partida 1

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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 infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado,	Evento	7 días hábiles posteriores a la solicitud generada por parte del Instituto

REC. de los integrantes del Consorcio:
 Participante A: CAS121106682
 Participante B: SU3C01239119
 Participante C: B57110223521



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	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 para el proceso de análisis	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto
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	Evento	15 días hábiles posteriores a la solicitud generada por parte del Instituto



CONSEJO FEDERAL DE ELECTRICIDAD Y ENERGÍA
 INSTITUTO FEDERAL DE PROTECCIÓN DE DATOS PERSONALES
 SECRETARÍA DE ECONOMÍA

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	de activos de infraestructura verificados		
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 (código) 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), de manera enunciativa más no limitativa, generará entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

Partida 1

NO PARTICIPA EL CONSORCIO, EN ESTA PARTIDA

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	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SDA300228919
 Participante C: 55721032821

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	de seguridad implementados		
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
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, serán entregados en formato electrónico (MS Word, MS Excel, PDF) conforme los periodos estipulados por el Instituto.

De igual manera, EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 funcionarios que sean designados por el primero mencionado.

13. Condiciones de aceptación de los servicios

1. Se formalizarán 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.

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: S543031348HE
 Participante C: B572109352L



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

14. Lugar y horario para la entrega

- 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.
- 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 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

EL CONSORCIO presenta escrito de confidencialidad.

16. Propiedad Intelectual

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 ponderación 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 Osmary Verdín 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.



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
 Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), generará 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

24. Otorgamiento de anticipo

No aplica

Protesto lo necesario

ATENTAMENTE

JULIO CRUZ GÓMEZ

APODERADO LEGAL DE CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.
 Y REPRESENTANTE COMÚN DEL CONSORCIO CONFORMADO POR CONSULTING ALL SERVICE IN TELECOM
 AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V.



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Manifiesto de Confidencialidad

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
 P r e s e n t e

EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), suscribirá el Convenio de Confidencialidad y Resguardo de Información Correspondiente con la persona designada como Administradora de Contrato. En complemento, EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), considerará al menos los siguientes mecanismos de control de acceso a la información del IMSS:

- a. Se establecerán controles de acceso y privilegios restringidos al personal de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del IMSS.
- b. EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), implantará y aceptará en todo momento el uso de controles que permitan "Pistas de Auditoría" 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), y las del IMSS.
- d. EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), contará con sistemas que contengan una administración estricta de registros y políticas de retención de la información del IMSS.
- e. Los empleados de EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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 EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), serán restringidos y observarán las políticas de seguridad del IMSS al respecto.
- h. EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), permitirá el acceso a información relacionada con el servicio prestado al IMSS para la realización de auditorías.
- i. EL CONSORCIO, en caso de resultar adjudicado de SASI 2022-2024 (partida 2), 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.



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- j. 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 CONSORCIO se obliga a utilizarlas exclusivamente para cubrir los servicios requeridos.
- k. EL CONSORCIO presenta como parte de su propuesta técnica, el presente escrito firmado por el suscrito 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.

ATENTAMENTE

JULIO CRUZ GÓMEZ

APODERADO LEGAL DE CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.
Y REPRESENTANTE COMÚN DEL CONSORCIO CONFORMADO POR CONSULTING ALL SERVICE IN TELECOM
AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V.

SIN TEXTO

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

III b). - Plan de trabajo propuesto

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

Me refiero al procedimiento de **Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022** en el que EL CONSORCIO participa a través de la presente propuesta.

Sobre el particular, manifestamos que integramos en nuestra propuesta técnica lo siguiente:

Plan de Trabajo para la atención del servicio objeto del servicio descrito en el Anexo Técnico y Apéndices (Partida 2), este incluye la transcripción íntegra y detallada del Anexo Técnico, Términos y Condiciones y Apéndices, así como la manifestación de aceptación y cumplimiento de los mismos, dicha información incluye la descripción amplia y detallada del servicio administrado de seguridad informática, así como la descripción de forma detallada de las especificaciones técnicas y de calidad solicitadas.

Este plan de trabajo incluye de manera enunciativa al menos lo siguiente:

- A. actividades a realizar.
- B. secuencia.
- C. responsables de las actividades.
- D. duración del servicio.
- E. fecha de inicio.
- F. fecha de conclusión.

Protesto lo necesario

ATENTAMENTE


JULIO CRUZ GÓMEZ

APODERADO LEGAL DE CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.
Y REPRESENTANTE COMÚN DEL CONSORCIO CONFORMADO POR CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V.

SIN TEXTO

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRES, 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

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	2014		2024		2029	
0		PLAN MACRO de trabajo SLABS IMSS Caillit	730 días	mar 01/11/22	lun 17/02/25						
1		1. INICIO	1 día	mar 01/11/22	mar 01/11/22						
2		Workshop previo KickOff	1 día	mar 01/11/22	mar 01/11/22						
3		KickOff	1 día	mar 01/11/22	mar 01/11/22						
4		2. PLANEACIÓN	1 día	mar 01/11/22	mar 01/11/22						
5		Solicitud de Requerimientos	1 día	mar 01/11/22	mar 01/11/22						
6		Usuarios para pruebas de caja blanca	1 día	mar 01/11/22	mar 01/11/22						
7		VPNs	1 día	mar 01/11/22	mar 01/11/22						
8		Aprobación de Plan de Trabajo	1 día	mar 01/11/22	mar 01/11/22						
9		Aprobación de SOW	1 día	mar 01/11/22	mar 01/11/22						
10		Supervisión de actividades	0 días	mar 01/11/22	mar 01/11/22						
11		Restricciones	2 horas	mar 01/11/22	mar 01/11/22						
12		3. EJECUCIÓN	60 días	mar 01/11/22	lun 09/01/23						
13		Análisis de Vulnerabilidades y Pruebas de Intrusión	60 días	mar 01/11/22	lun 09/01/23						
14		Externas (CAJA NEGRA)	60 días	mar 01/11/22	lun 09/01/23						
15		Caja Negra	60 días	mar 01/11/22	lun 09/01/23						
16		Desdoblamiento	10 días	mar 01/11/22	vie 11/11/22						
17		Evaluación (DEPENDIE EL UNIVERSO DE EQUIPOS)	60 días	mar 01/11/22	lun 09/01/23						
18		Exploración	15 días	mar 01/11/22	jue 17/11/22						
19		Supervisión de actividades	0 días	mar 01/11/22	mar 01/11/22						
20		Internas (CAJA GRIS Y BLANCA)	40 días	mar 01/11/22	vie 16/12/22						
21		Caja Gris	10 días	mar 01/11/22	vie 11/11/22						
22		Desdoblamiento	10 días	mar 01/11/22	vie 11/11/22						
23		Evaluación	10 días	mar 01/11/22	vie 11/11/22						
24		Exploración	10 días	mar 01/11/22	vie 11/11/22						
25		Supervisión de actividades	0 días	mar 01/11/22	mar 01/11/22						
26		Caja Blanca	30 días	lun 14/11/22	vie 16/12/22						
30		Realización de Informe Ejecutivo	10 días	mar 01/11/22	vie 11/11/22						
31		Realización Informe Técnico Detallado	10 días	mar 01/11/22	vie 11/11/22						
32		Supervisión de actividades	0 días	mar 01/11/22	mar 01/11/22						
33		Análisis de código estático	16.13 días	mar 01/11/22	vie 18/11/22						
34		Definición de una aplicación a evaluar por monex	1 día	mar 01/11/22	mar 01/11/22						
35		Contexto de aplicación	0.38 días	mar 01/11/22	mar 01/11/22						

SIN TEXTO

Id	Módulo	Nombre de tarea	Duración	Comienzo	Fin	Año		
						2014	2019	2024
36	36	Ejecución del servicio	5 días	mar 01/11/22	lun 07/11/22			2029
37	37	Generación de Reporte de Hallazgos	16.13 días	mar 01/11/22	vie 18/11/22			
38	38	Supervisión de actividades	0 días	mar 01/11/22	mar 01/11/22			
39	39	Acompañamiento a Mitigación de Vulnerabilidades	6 días	vie 18/11/22	lun 28/11/22			
42	42	Análisis de flujo de proceso.	22 días	mar 01/11/22	lun 28/11/22			
43	43	Entendimiento	1 día	mar 01/11/22	mar 01/11/22			
44	44	Entrevistas y verificación de controles	8 días	mar 01/11/22	jue 10/11/22			
45	45	Identificación de riesgos	3 días	mar 01/11/22	vie 04/11/22			
46	46	Generación de reporte	22 días	mar 01/11/22	lun 28/11/22			
47	47	Supervisión de actividades	0 días	mar 01/11/22	mar 01/11/22			
48	48	Certificación/ Re-escaneo de Vulnerabilidades	30 días	mar 01/11/22	mar 06/12/22			
49	49	Análisis Forense	73 días	mar 01/11/22	lun 23/01/23			
50	50	Identificación, entendimiento del incidente y atención del Requerimiento	73 días	mar 01/11/22	lun 23/01/23			
51	51	Busqueda y recuperación de evidencia digital	10 días	mar 01/11/22	vie 11/11/22			
52	52	Preservación de la evidencia digital	10 días	mar 01/11/22	vie 11/11/22			
53	53	Análisis de la evidencia digital	10 días	mar 01/11/22	vie 11/11/22			
54	54	Documentación	10 días	mar 01/11/22	vie 11/11/22			
55	55	Presentación de resultados	1 día	mar 01/11/22	mar 01/11/22			
56	56	Destrucción de copias de trabajo y Almacenamiento (o devolución de evidencia digital)	1 día	mar 01/11/22	mar 01/11/22			
57	57	Supervisión de actividades	0 días	mar 01/11/22	mar 01/11/22			
58	58	Supervisión	730 días	mar 01/11/22	lun 17/02/25			
59	59	Revisión SLA's	730 días	mar 01/11/22	lun 17/02/25			
60	60	Escalación de Issues y riesgos	730 días	mar 01/11/22	lun 17/02/25			
61	61	Reporte Ejecutivo de avance	730 días	mar 01/11/22	lun 17/02/25			
62	62	Cierre	639.13 días	mar 01/11/22	vie 01/11/24			
63	63	Presentación de Hallazgos	1 día	mar 01/11/22	mar 01/11/22			
64	64	Entregables del proyecto	30 días	mar 01/11/22	mar 06/12/22			
65	65	Acta de cierre de proyecto	1 día	vie 01/11/24	vie 01/11/24			

C:\Program Files\Microsoft Office\Office16\Wordpad.exe
 Microsoft Word - ANEXOS
 Microsoft Word - ANEXOS

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRES, 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

SIN TEXTO



CALLIT
SOLUTION KNOWLEDGE

callit.com.mx
contacto@callit.com.mx
Of. +52 55 118702
Río Rhin #22 interior 504
Col. Cuauhtémoc, CDMX

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

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 2			
No.	Descripción de Servicio	Unidad de Medida	Precio Unitario
49	Análisis de Vulnerabilidades Estático	Servicio	\$32,142.86
50	Análisis de Vulnerabilidades Dinámico	Servicio	\$11,160.71
51	Pruebas de Penetración	Servicio	\$17,857.14
52	Análisis Forense	Servicio	\$142,857.14
Suma de Precios Unitarios:			\$204,017.85

Monto en letra sin IVA (Doscientos cuatro mil diecisiete pesos 85/100 M.N.)

- Precios serán fijos durante la vigencia del contrato

Razón Social: CONSORCIO CONFORMADO POR CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V.

RFC: CAS121106653, BST2103235Z1, SLA2001239H9

Lugar y fecha: Ciudad de México, a 30 de septiembre de 2022

Representante Legal del Licitante Julio Cruz Gómez

Protesto lo necesario

ATENTAMENTE


JULIO CRUZ GÓMEZ

APODERADO LEGAL DE CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.
Y REPRESENTANTE COMÚN DEL CONSORCIO CONFORMADO POR CONSULTING ALL SERVICE IN
TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS,
S.A. DE C.V.

Río Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-0500CYR019-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-0500CYR019-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 Requiriente 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-050QYR019-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-050QYR019-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 Requiriente 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-E1B2-2022

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

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050CYR019-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 fórmula: -----

$$PPE = MPemb \times 40 / MPI$$

Donde: -----

PPE = Puntuación que corresponde a la Propuesta Económica; -----

MPemb = Precio Unitario ofertado más bajo, y -----

MPI = 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	$92,657,867 \times 40 = 3,706,314,680$ $3,706,314,680 / 92,657,867 = 40$	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	$92,657,867 \times 40 = 3,706,314,680$ $3,706,314,680 / 128,819,681 = 28.77$	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.-	Axtef, S.A.B. de C.V.	\$797,897.29	$149,412.54 \times 40 = 5,976,501.60$ $5,976,501.60 / 797,897.29 = 7.49$	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	$149,412.54 \times 40 = 5,976,501.60$ $5,976,501.60 / 204,017.85 = 29.29$	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	$149,412.54 \times 40 = 5,976,501.60$ $5,976,501.60 / 149,412.54 = 40$	40.00
4.-	Scitum S.A. de C.V.	\$513,561.00	$149,412.54 \times 40 = 5,976,501.60$ $5,976,501.60 / 513,561 = 11.64$	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	$149,412.54 \times 40 = 5,976,501.60$ $5,976,501.60 / 298,190.90 = 20.04$	20.04

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA

NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050CYR039-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:

$$PT_j = TPT + PPE \text{ Para toda } j = 1, 2, \dots, n$$

Dónde:

PT_j = 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 Silent4Business, 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	AxteI, 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.

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 Medicine 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.II.- 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-formalizacion-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 1º de junio de 2022, se señalan los datos de los contratos derivados del presente procedimiento conforme a 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.

Partida 1 Datos del contrato y su garantía	
Licitante adjudicado: Operbes, S.A. de C.V., en participación conjunta con Silent4Bussines, S.A. de C.V. y Bufete Empresarial CTI, 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	
Licitante adjudicado: Consulting All Service in Telecom And Medicine 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:-----

ACTA DE FALLO

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA
NÚMERO DE IDENTIFICACIÓN EN COMPRANET: LA-050GYR019-EI82-2022
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.

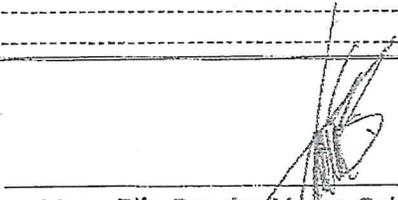
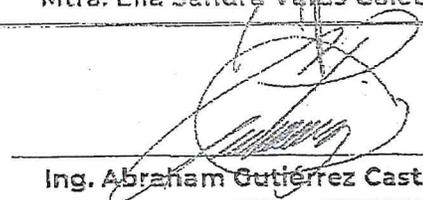
4.2.2.1.15, 4.2.2.1.16 y 4.2.2.1.17 del Acuerdo por el que se expide el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público. -----

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: -----

<p>Titular de la División de Contratación de Activos y Logística (Área Contratante)</p>	 <p>Mtra. Elia Sandra Vargas Galeana</p>
<p>Titular de la División de Seguridad Informática Física (Área Requiriente y Técnica)</p>	 <p>Ing. Abraham Gutiérrez Castillo</p>
<p>Representante de la Coordinación de Legislación y Consulta</p>	 <p>Lic. Mayra Selene García Aguilar</p>
<p>Representante del Órgano Interno de Control en el IMSS</p>	 <p>Lic. Sergio Emilio Segura Ortega</p>

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



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

CONTRATO
NÚMERO
019E18222-002

ANEXO 4 (CUATRO)

“DOCUMENTO DE DESIGNACIÓN DE ADMINISTRADOR DEL CONTRATO”

**ANEXOS
DIVISIÓN DE CONTRATOS**

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

SIN TEXTO

Of N° 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
Presente

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



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 PLANEACIÓN Y CONTRATOS

CONTRATO
NÚMERO
019E18222-002

ANEXO 5 (CINCO)

**“JUNTA DE ACLARACIONES, LA CUAL SE ENCUENTRA DISPONIBLE
PARA SU CONSULTA EN COMPRANET”**

SIN TEXTO

GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Planeación y Contratos
División de Contratos

“JUNTA DE ACLARACIONES DISPONIBLE PARA SU CONSULTA EN EL PORTAL DE COMPRAS GUBERNAMENTALES COMPRANET”

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 PLANEACIÓN Y CONTRATOS

CONTRATO
NÚMERO
019E18222-002

ANEXO 6 (SEIS)

“CONVENIO DE PARTICIPACIÓN CONJUNTA”

**ANEXOS
DIVISIÓN DE CONTRATOS**

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

SIN TEXTO

PA-11



CALLIT

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Convenio de Participación Conjunta

RFC de los integrantes del Consorcio:
Participante A: CAS121106653
Participante B: SLA2001239H9
Participante C: BST2103235Z1

ANEXOS
DIVISIÓN DE CONTRATOS

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX
Tel: 55118702; correo: julio.cruz@callit.com.mx
Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.
RFC: CAS121106653



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022
Anexo 15.- Modelo de convenio de proposición conjunta

CONVENIO DE PROPOSICIÓN CONJUNTA QUE CELEBRAN POR UNA PARTE CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., REPRESENTADA POR JULIO CRUZ GÓMEZ EN SU CARÁCTER DE APODERADO LEGAL, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ "EL PARTICIPANTE A", POR OTRA SECURE LABS, S.A. DE C.V., REPRESENTADA POR ALBERTO VARGAS MAGAÑA, EN SU CARÁCTER DE APODERADO LEGAL, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ "EL PARTICIPANTE B", Y POR OTRA BOHMER STRATEGISTS, S. DE R. L. DE C.V., REPRESENTADA POR [REDACTED]

[REDACTED] EN SU CARÁCTER DE PRESIDENTE DEL CONSEJO DE GERENTES, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ "EL PARTICIPANTE C", Y CUANDO SE HAGA REFERENCIA A LOS QUE INTERVIENEN SE DENOMINARÁN "Las Partes", AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS.

1.1. "EL PARTICIPANTE A", DECLARA QUE.:

1.1.1 ES UNA SOCIEDAD LEGALMENTE CONSTITUIDA, DE CONFORMIDAD CON LAS LEYES MEXICANAS, SEGÚN CONSTA EN EL TESTIMONIO DE LA ESCRITURA PÚBLICA (PÓLIZA) NÚMERO 268,140, DE FECHA 06 DE NOVIEMBRE DE 2012, OTORGADA ANTE LA FE DEL LIC. CLAUDIO JUAN RAMÓN HERNÁNDEZ DE RUBÍN, NOTARIO PÚBLICO NÚMERO 123, DEL DISTRITO FEDERAL (HOY CIUDAD DE MÉXICO), E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DE COMERCIO DEL DISTRITO FEDERAL (HOY CIUDAD DE MÉXICO), EN EL FOLIO MERCANTIL 483,484-1 DE FECHA 15 DE NOVIEMBRE DEL 2012.

EL ACTA CONSTITUTIVA DE LA SOCIEDAD SI HA TENIDO REFORMAS Y MODIFICACIONES:

- REFORMA 1, INSTRUMENTO NO. 31,162 DE FECHA 10 DE OCTUBRE DE 2016, OTORGADA ANTE EL NOTARIO PÚBLICO LIC. PEDRO BERNARDO BARRERA CRISTIANI, NOTARIO PÚBLICO NÚMERO 82 DE LA CIUDAD DE MÉXICO REGISTRO PÚBLICO DE LA PROPIEDAD NO. 483484 -1.
- REFORMA 2, INSTRUMENTO NO. 28,411 DE FECHA 31 DE MAYO DE 2019, OTORGADA ANTE EL NOTARIO PÚBLICO LIC. PEDRO JOAQUÍN ROMANO ZARRABE, NOTARIO PÚBLICO NÚMERO 123 DE LA CIUDAD DE MÉXICO REGISTRO PÚBLICO DE LA PROPIEDAD NO. 483484 -1.

LOS NOMBRES DE SUS SOCIOS SON:

SOCIO	RFC
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

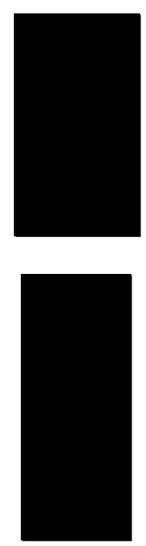
1.1.2 TIENE LOS SIGUIENTES REGISTROS OFICIALES. REGISTRO FEDERAL DE CONTRIBUYENTES NÚMERO CAS121106653 Y REGISTRO PATRONAL ANTE EL INSTITUTO MEXICANO DEL SEGURO SOCIAL NÚMERO [REDACTED]

1.1.3 SU REPRESENTANTE LEGAL CON EL CARÁCTER YA MENCIONADO, CUENTA CON LAS FACULTADES NECESARIAS PARA SUSCRIBIR EL PRESENTE CONVENIO, DE CONFORMIDAD CON EL CONTENIDO DEL TESTIMONIO DE LA ESCRITURA PÚBLICA NÚMERO 31,188 DE FECHA 20 DE OCTUBRE DE 2016, OTORGADA ANTE LA FE DEL LIC. PEDRO BERNARDO BARRERA CRISTIANI NOTARIO PÚBLICO NÚMERO 82, DE LA CIUDAD DE MÉXICO E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DE

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE DE SOCIO, RFC, NOMBRE Y FIRMA, 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

RFC de los integrantes del Consorcio:
Participante A: CAS121106653
Participante B: SLA200123949
Participante C: BS1210929521



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

COMERCIO, EN EL FOLIO MERCANTIL NÚMERO 483,484-1, DE FECHA 15 DE NOVIEMBRE DEL 2012., MANIFESTANDO "BAJO PROTESTA DE DECIR VERDAD", QUE DICHAS FACULTADES NO LE HAN SIDO REVOCADAS, NI LIMITADAS O MODIFICADAS EN FORMA ALGUNA, A LA FECHA EN QUE SE SUSCRIBE EL PRESENTE INSTRUMENTO JURÍDICO.

EL DOMICILIO DEL REPRESENTANTE LEGAL ES EL UBICADO EN: [REDACTED]

1.1.4 SU OBJETO SOCIAL, ENTRE OTROS CORRESPONDE A.

Descripción del Objeto Social.

1. La prestación de todo tipo de servicios públicos de telecomunicaciones y/o radiodifusión previa concesión, autorización, o similar que en su caso otorgue el Instituto Federal de Telecomunicaciones y/o cualquier autoridad competente.
2. La instalación, operación, explotación o comercialización de una red pública de telecomunicaciones.
3. Usar, aprovechar y explotar bandas de frecuencia del espectro radioeléctrico de uso determinado y para la ocupación y explotación de recursos orbitales; ya sea para uso comercial, público, privado o social
4. Otorgar en arrendamiento las bandas de frecuencia para uso comercial o privado, previa autorización que otorgue el Instituto Federal de Telecomunicaciones y/o cualquier autoridad competente.
5. La instalación, operación o explotación de estaciones terrenas transmisoras.
6. La transmisión o emisión de señales, datos, imágenes, voz, sonidos o informaciones de cualquier naturaleza ya sea por sistemas alámbricos o inalámbricos, por satélite, medios ópticos o cualquier otro sistema o media de transmisión conocido o por conocer.
7. El uso, aprovechamiento y explotación de los servicios especiales de telecomunicaciones que sean auxiliares a las vías generales de comunicación o de explotaciones domésticas, industriales, agrícolas, mineras, comerciales o de otra índole.
8. Establecer y operar o explotar una comercializadora de servicios de telecomunicaciones sin tener el carácter de concesionario.
9. La comercialización, producción, fabricación, importación y exportación de toda clase de productos y en especial la instalación, compra y venta de equipos de cómputo y médicos, telefónicos, comunicación software, paquetería en general, accesorios periféricos, consumibles y sistemas de cómputo, así como toda clase de cables y equipo relacionado con telecomunicaciones, construcciones civiles, instalaciones eléctricas, mantenimiento a edificios en general, construcción de canalización, contratación de mantenimientos de equipos electrónicos y eléctricos para comunicaciones y cómputo y venta de equipos electrónicos para la medición en las obras civiles, así como la elaboración de contratos relacionados con este objeto; pólizas y servicios de mantenimiento preventivo y correctivo de equipos de cómputo y equipos de telecomunicaciones, de todo tipo de sistemas y redes de telecomunicación y la prestación de toda clase de servicios, a cualquier persona física o moral de naturaleza privada o pública.

Por lo que enunciativa pero no limitativamente, la sociedad podrá:

- I. Ejecutar toda clase de actos de comercio pudiendo comprar, vender, adquirir, distribuir, importar, exportar, producir, fabricar, manufacturar, transformar, maquilar, comercializar y en general, negociar con toda clase de artículos y mercancías por cuenta propia o ajena, en la República Mexicana o en el Extranjero.
- II. Prestar y recibir toda clase de servicios legales, fiscales, de contabilidad, administrativos y de asesoría en general, a empresas en la República Mexicana o en el Extranjero.
- III. Llevar a cabo por cuenta propia o de terceros programas de capacitación y desarrollo, así como investigaciones científicas para desarrollo tecnológico o investigaciones profesionales, en las materias que requieran las personas físicas o morales a las que la sociedad preste servicios o a las que la propia sociedad considere conveniente, ya sea directamente o por medio de Institutos Tecnológicos y Universitarios o empresas o instituciones especializadas en el País o en el Extranjero o mediante asociación con dichos

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA200123949
 Participante C: BST210323521

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx;

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653

ANEXOS

DIVISIÓN DE CONTRATACIÓN



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

institutos, universidades, empresas o instituciones especializadas y proporcionar a sus clientes los resultados de dicha investigación.

- IV. Obtener, adquirir, registrar, utilizar o disponer de toda clase de patentes, marcas industriales y de servicio, certificados de invención o nombres comerciales, diseños y dibujos industriales, derechos de autor y cualquier otro tipo de derechos de propiedad industrial, literaria o artística y derechos sobre ellos ya sea en México o en el Extranjero.
V. Obtener por cualquier título, concesiones, permisos, autorizaciones o licencias, así como celebrar cualquier clase de contratos, con la administración pública sea federal o local o con cualquier particular
VI. Dar o tomar dinero en préstamo con o sin garantía, emitir bonos, obligaciones, (así), valores y otros títulos de crédito, así como adquirir legalmente y negociar con bonos, obligaciones, acciones, valores y otros títulos de crédito emitidos por terceros.
VII. Otorgar avales y obligarse solidariamente, así como constituir garantías a favor de terceros.
VIII. Realizar la construcción, administración y operación de servicios y recursos de centros de operación de redes (NOC), Centro de Operaciones de seguridad (SOC) y mesas de servicios técnicos y operativos relacionados con la fabricación de software y recursos asociados.
IX. Prestar el servicio de consultoría para el diagnóstico de problemas en el área de telecomunicaciones y conectividad, optimización de herramientas para la red de voz, referente a tecnologías de la información o telecomunicaciones, antenas, radios, router, black bond, gabinetes entre otros.
X. Comprar, vender, comercializar y prestar servicios de mantenimiento e instalación de todo tipo de equipo referente a tecnologías de la información de telecomunicaciones tales como antenas, radios, gabinetes entre otros, necesarios para optimizar todo tipo de dispositivos de comunicación y transferencia de datos, de voz, imagen y multimedia.
XI. Comprar, vender, comercializar y prestar el servicio de mantenimiento de equipos de sonido y espectáculos; prestar el servicio de banquetes, meseros y comida a todo tipo de personas tanto públicas como privadas.
XII. Comprar, vender, comercializar y prestar servicios de mantenimiento de todo tipo de equipos para la generación de energía eléctrica a través de todo tipo de fuentes ordinarias o alternativas, tales como la solar, eólica, geotérmica etc.
XIII. Formar parte directa o indirectamente de otras sociedades o asociaciones e intervenir en todos los asuntos y derechos relacionados con ellas
XIV. Establecer sucursales, oficinas, subsidiarias y agencias, así como representar o ser agente de empresas e intermediar en la venta de toda clase de bienes y servicios
XV. Adquirir o poseer por cualquier título, usar, dar o tomar en arrendamiento, administrar, vender o disponer en cualquier forma, de todos los bienes muebles o inmuebles, así como derechos reales o personales sobre ellos, que fueren necesarios o convenientes para la realización del objeto de la sociedad.
XVI. Contratar al personal necesario.
XVII. En general celebrar toda clase de contratos ya sean civiles, mercantiles o de cualquier naturaleza

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR 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

POR LO QUE CUENTA CON LOS RECURSOS FINANCIEROS, TÉCNICOS, ADMINISTRATIVOS Y HUMANOS PARA OBLIGARSE, EN LOS TÉRMINOS Y CONDICIONES QUE SE ESTIPULAN EN EL PRESENTE CONVENIO.

2.1 "EL PARTICIPANTE B", DECLARA QUE:

2.1.1 ES UNA SOCIEDAD LEGALMENTE CONSTITUIDA DE CONFORMIDAD CON LAS LEYES DE LOS ESTADOS UNIDOS MEXICANOS, SEGÚN CONSTA EL TESTIMONIO (PÓLIZA) DE LA ESCRITURA PÚBLICA NÚMERO 122,833 DE FECHA 23 DE ENERO DE 2020 PASADA ANTE LA FE DEL DR. OTHON PÉREZ FERNÁNDEZ DEL CASTILLO, NOTARIO PÚBLICO NÚMERO 63 DE LA CIUDAD DE MÉXICO E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DEL COMERCIO, EN EL FOLIO MERCANTIL NÚMERO N-2020018436 DE FECHA 23 DE MARZO DE 2020.

RFC de los integrantes del Consorcio:
Participante A: CAS121106653
Participante B: SAZ001239H9
Participante C: B572103235Z1

[Handwritten signature]



[Handwritten signature]



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

EL ACTA CONSTITUTIVA DE LA SOCIEDAD NO HA TENIDO REFORMAS Y MODIFICACIONES.

Nota. En su caso, se deberán relacionar las escrituras en que consten las reformas o modificaciones de la sociedad.

LOS NOMBRES DE SUS SOCIOS SON:

SOCIO	RFC
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

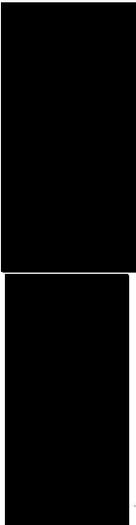
2.1.2 TIENE LOS SIGUIENTES REGISTROS OFICIALES. REGISTRO FEDERAL DE CONTRIBUYENTES NÚMERO SLA2001239H9 Y REGISTRO PATRONAL ANTE EL INSTITUTO MEXICANO DEL SEGURO SOCIAL NÚMERO [REDACTED]

2.1.3 SU REPRESENTANTE LEGAL, CON EL CARÁCTER YA MENCIONADO, CUENTA CON LAS FACULTADES NECESARIAS PARA SUSCRIBIR EL PRESENTE CONVENIO, DE CONFORMIDAD CON EL CONTENIDO DEL TESTIMONIO DE LA ESCRITURA PÚBLICA NÚMERO 122,833 DE FECHA 23 DE ENERO DE 2020 PASADA ANTE LA FE DEL DR. OTHON PÉREZ FERNÁNDEZ DEL CASTILLO, NOTARIO PÚBLICO NÚMERO 63 DE LA CIUDAD DE MÉXICO E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DEL COMERCIO, EN EL FOLIO MERCANTIL NÚMERO N-2020018436 DE FECHA 23 DE MARZO DE 2020, MANIFESTANDO "BAJO PROTESTA DE DECIR VERDAD" QUE DICHAS FACULTADES NO LE HAN SIDO REVOCADAS, NI LIMITADAS O MODIFICADAS EN FORMA ALGUNA, A LA FECHA EN QUE SE SUSCRIBE EL PRESENTE INSTRUMENTO JURÍDICO.

EL DOMICILIO DE SU REPRESENTANTE LEGAL ES EL UBICADO EN [REDACTED]

2.1.4 SU OBJETO SOCIAL, ENTRE OTROS CORRESPONDE A:

- a) Elaboración, compra, venta, distribución, comercialización, implantación, desarrollo, ejecución y en general llevar a cabo todo tipo de actividades relacionadas con programas de computación, sistemas de información, servicios tecnológicos de seguridad, sistemas de animación digital, implantación de lenguajes y redes para computadoras y cualquier tipo de medios electrónicos, así como el establecimiento de sitios electrónicos, incluyendo aquellos accesibles vía redes de comunicación incluyendo, entre otros, el Internet.
- b) Importación y exportación de programas, sistemas de información, sistemas de comunicación y redes de computadoras.
- c) Consultoría y asesoría técnica y profesional a personas físicas o morales nacionales o extranjeras en la implantación, desarrollo y ejecución de los programas, juegos y video, sistemas de la información, implantación de lenguajes y redes para computadora.
- d) Llevar a cabo por cuenta propia o de terceros, servicios de información, publicidad y mercadotecnia, así como todo tipo de compra, desarrollo y venta de programas de computación.



[Handwritten signature]

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y RFC DE SOCIO, DOMICILIO, NOMBRE Y FIRMA, 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: NOMBRE Y RFC DE SOCIO DE EMPRESA, 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

RFC de los integrantes del Consorcio:
Participante A: CAS121106653
Participante B: SLA2001239H9
Participante C: 851210323521



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- e) Llevar a cabo por cuenta propia o de terceros, programas de capacitación y desarrollo así como investigaciones científicas para desarrollo tecnológico o investigaciones profesionales en las materias que requieran las personas físicas o morales a las que la Sociedad considere conveniente ya sea directamente o por medio de institutos tecnológicos, universidades, empresas o instituciones especializadas y proporcionar a sus clientes los resultados de dicha investigación.
- f) Elaboración, desarrollo y ejecución de toda clase de programas para computadoras, supervisión y seguimiento en el desarrollo de los mismos.
- g) Importación, exportación, compraventa y arrendamiento de toda clase de tecnología necesaria para la elaboración de programas, sistemas de información, sistemas de comunicaciones, implantación de lenguajes y redes para computadoras.
- h) Prestación de servicios de asesoría técnica y administrativa en la ejecución de los programas, lenguajes, sistemas y redes de computación elaborados e implantados por la sociedad.
- i) El arrendamiento, comercialización, fabricación, importación, exportación, distribución, representación, reconstrucción, almacenaje, operación, industrialización, mantenimiento, comisión, compra, venta, consignación, administración, permuta, comodato, en general en todas sus formas con toda clase de materias primas, insumos, materiales, productos, artículos, maquinaria, equipo y bienes de cualquier clase, especie y descripción en general.
- j) Registrar, adquirir, obtener, conceder, poseer, usar, administrar, explotar, licenciar, disponer y negociar bajo cualquier medio, título o concepto permitido por la ley, toda clase de tecnología nacional o extranjera, así como toda clase de derechos de autor, de patentes, marcas, nombres y avisos comerciales, invenciones, derechos de propiedad industrial, mejoras, modelos o dibujos industriales, signos distintivos, procesos industriales y licencias.
- k) La obtención, adquisición y transferencia por cualquier título legal de concesiones y franquicias.
- l) La prestación y contratación de servicios personales, profesionales, de administración, comisión, mediación, distribución, representación, mantenimiento, asesoría, ejecución de proyectos y en general cualquier otro permitido por la ley.
- m) La participación en el capital social de cualquier tipo de sociedades mercantiles o civiles, con la consecuente suscripción de partes sociales o acciones y la enajenación de las mismas por cualquier título legal.
- n) La constitución, organización, promoción y administración de toda clase de sociedades mercantiles o civiles, así como la adquisición, enajenación, custodia y realización de toda clase de actos jurídicos con acciones, certificados de participación, bonos, obligaciones, partes sociales y toda clase de títulos-valor.
- o) Actuar como y designar contratistas, comisionistas, distribuidores, representantes, mediadores o agentes.
- p) Adquirir, enajenar, arrendar, subarrendar, usar y otorgar el uso, goce, disposición o en general la explotación de toda clase de bienes muebles o inmuebles, incluyendo sus partes o accesorios, así como cualquier tipo de derechos reales sobre los mismos, que resulten necesarios o convenientes para cumplir con los fines de la Sociedad.
- q) Dar o tomar dinero en préstamo con o sin garantía, emitir a cienes, obligaciones, cédulas hipotecarias, valores y otros títulos de crédito, con la intervención de las instituciones señaladas por la ley, así como adquirir legalmente y negociar con bonos, obligaciones, acciones, cédulas hipotecarias, valores títulos de crédito emitidos por terceros y en general, adquirir y negociar con toda clase de efectos de comercio y otorgar las garantías que fueren necesaria para realizar los objetos de la sociedad.

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

RFC de los integrantes del Consortio:
 Participante A: CAS121106653
 Participante B: SJA2001239H9
 Participante C: B87210323521

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- r) Recibir y ejecutar los poderes y mandatos que le otorgaren las personas físicas o morales a los que prestare servicio y delegar en su caso el ejercicio de dichos poderes o mandatos.
- s) Establecer sucursales, oficinas de representación y corresponsalías en cualquier parte de la República Mexicana o del extranjero así como señalar y someterse a domicilios convencionales.
- t) Promover, organizar, constituir, administrar, operar y supervisar toda clase de sociedades mercantiles o civiles ya sea en la República Mexicana o en el extranjero.
- u) Ser proveedor, cliente o contratista del Gobierno Federal. así como de gobiernos Estatales o Municipales.
- v) Otorgar y suscribir títulos de crédito, aceptarlos, endosarlos y negociarlos, constituirse como obligado solidario o aval y, en general, otorgar cualquier tipo de garantías tanto en los negocios que realice la sociedad como a favor de terceras personas físicas o morales.
- w) Además, la celebración de todos los contratos, convenios, acuerdos, documentos y la ejecución de la totalidad de los actos, civiles, mercantiles y de cualquier tipo dentro del marco legal. relacionados, necesarios, o convenientes para el desarrollo de su objeto social o que sean medios o consecuencia del mismo, por lo cual, la sociedad podrá hacer, celebrar, suscribir y participar en todos los actos a los que pueda dedicarse legítimamente una Sociedad Anónima de Capital Variable.

POR LO QUE CUENTA CON LOS RECURSOS FINANCIEROS, TÉCNICOS, ADMINISTRATIVOS Y HUMANOS PARA OBLIGARSE, EN LOS TÉRMINOS Y CONDICIONES QUE SE ESTIPULAN EN EL PRESENTE CONVENIO.

3.1 "EL PARTICIPANTE C", DECLARA QUE:

3.1.1 ES UNA SOCIEDAD LEGALMENTE CONSTITUIDA DE CONFORMIDAD CON LAS LEYES DE LOS ESTADOS UNIDOS MEXICANOS, SEGÚN CONSTA LA PÓLIZA DE LA ESCRITURA PÚBLICA NÚMERO 1971 DE FECHA 1 DE MARZO DE 2021 PASADA ANTE LA FE DEL LIC. CARLOS LUVIANO MONTELONGO CORREDOR PÚBLICO NÚMERO 64 DE LA PLAZA DE JALISCO E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DEL COMERCIO, EN EL FOLIO MERCANTIL NÚMERO N-2021021629 DE FECHA 06/04/2021.

EL ACTA CONSTITUTIVA DE LA SOCIEDAD NO HA TENIDO REFORMAS Y MODIFICACIONES.

Nota. En su caso, se deberán relacionar las escrituras en que consten las reformas o modificaciones de la sociedad.

LOS NOMBRES DE SUS SOCIOS SON:

SOCIO	RFC
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

3.1.2 TIENE LOS SIGUIENTES REGISTROS OFICIALES. REGISTRO FEDERAL DE CONTRIBUYENTES NÚMERO BST2103235Z1 Y REGISTRO PATRONAL ANTE EL INSTITUTO MEXICANO DEL SEGURO SOCIAL NÚMERO [REDACTED]

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y RFC DE SOCIOS, NOMBRE Y FIRMA DE PERSONA FÍSICA, 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

RFC de los integrantes del Consorcio:
Participante A: CAS121106653
Participante B: SLA200123949
Participante C: BST2103235Z1



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

3.1.3 SU REPRESENTANTE LEGAL, CON EL CARÁCTER YA MENCIONADO, CUENTA CON LAS FACULTADES NECESARIAS PARA SUSCRIBIR EL PRESENTE CONVENIO, DE CONFORMIDAD CON EL CONTENIDO DE LA PÓLIZA DE LA ESCRITURA PÚBLICA NÚMERO 1971 DE FECHA 1 DE MARZO DE 2021 PASADA ANTE LA FE DEL LIC. CARLOS LUVIANO MONTELONGO CORREDOR PÚBLICO NÚMERO 64 DE LA PLAZA DE JALISCO E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DEL COMERCIO, EN EL FOLIO MERCANTIL NÚMERO N-2021021629 DE FECHA 06/04/2021, MANIFESTANDO "BAJO PROTESTA DE DECIR VERDAD" QUE DICHAS FACULTADES NO LE HAN SIDO REVOCADAS, NI LIMITADAS O MODIFICADAS EN FORMA ALGUNA, A LA FECHA EN QUE SE SUSCRIBE EL PRESENTE INSTRUMENTO JURÍDICO.

EL DOMICILIO DE SU REPRESENTANTE LEGAL ES EL UBICADO EN [REDACTED]

3.1.4 SU OBJETO SOCIAL, ENTRE OTROS CORRESPONDE A:

1. Ser intermediario distribuidor, comisionista, representante, mediador, agente, o con cualquier otro carácter de persona física o moral, nacionales o extranjeras e intermediar en la venta de toda clase de bienes y servicios.
2. Comprar, vender y en general comercializar toda clase de bienes, productos o servicios.
3. Comercialización, compra, venta, importación, exportación, industrialización, distribución, fabricación, representación, concesión, comisión, arrendamiento de toda clase de bienes, productos, servicios y servicios secundarios de valor agregado y el comercio en general con toda clase de equipos, servicios y productos.
4. La promoción, constitución, organización, explotación, adquisición y toma de participación en el capital social o patrimonio de todo tipo de sociedades mercantiles o civiles, asociaciones o empresas, de cualquier naturaleza y como quiera que se les denomine, ya sean industriales, comerciales, de servicios o de cualquier otra índole, tanto nacionales como extranjeras, así como participar en su administración.
5. La representación tanto en los Estados Unidos Mexicanos como en el extranjero, en calidad de agente, comisionista, intermediario, representante o mandatario, de toda clase de sociedades, empresas, negocios o personas físicas o morales, mexicanas o extranjeras, públicas o privadas, de cualquier naturaleza y como quiera que se les denomine.
6. La celebración de toda clase de contratos y convenios, así como la ejecución de toda clase de operaciones mercantiles y procedimientos jurídicos o actos profesionales en las áreas de negocio expresadas en los incisos anteriores, ya sea en nombre propio o en representación de terceros.
7. Contratar el personal necesario para el cumplimiento de los fines sociales y delegar en una o varias personas el cumplimiento de mandatos, comisiones, servicios y demás actividades propias de su objeto.
8. La obtención y aprovechamiento por cualquier medio legal de toda clase de concesiones, permisos, franquicias, licencias, autorizaciones, asignaciones, registros, patentes, marcas, derechos de autor, nombres y avisos comerciales que contribuyan a la realización del objeto y fines sociales de la Sociedad.
9. Recibir de otras sociedades y personas, así como proporcionar a otras sociedades y personas, los servicios que sean necesarios para el logro de sus finalidades u objetos sociales, tales como servicios administrativos, financieros, de tesorería, auditoría, mercadotecnia, contables,

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: DOMICILIO, NOMBRE Y FIRMA, 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

RFC de los integrantes del Consortio:
 Participante A: CAS121106653
 Participante B: SLA200123919
 Participante C: BST210323521



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

elaboración de programas y manuales, análisis de resultados de operación, evaluación de información sobre productividad y de posibles financiamientos, preparación de estudios acerca de la disponibilidad de capital, asistencia técnica, asesoría, consultoría, entre otros.

10. Obtener, adquirir, desarrollar, hacer mejoras, utilizar, otorgar y recibir licencias o disponer, conforme a cualquier título legal, de toda clase de patentes, marcas, modelos de utilidad, derechos de autor, diseños industriales, secretos industriales, certificados de invención, avisos y nombres comerciales, y cualesquiera otros derechos de propiedad industrial, ya sea en México o en el extranjero.
11. La obtención de toda clase de financiamientos, préstamos o créditos, emitir obligaciones, bonos, papel comercial y cualesquiera instrumentos de deuda o valores de deuda, como quiera que se les denomine y regidos por cualquier legislación, con o sin el otorgamiento de garantías reales, mediante prenda, hipoteca, fideicomiso o conforme a cualquier otro título legal, o que cuenten con garantías personales, para cualesquier fines que determine la Sociedad.
12. Otorgar cualquier tipo de financiamiento o préstamo a personas o sociedades mercantiles o civiles, empresas e instituciones.
13. Otorgar toda clase de garantías reales, personales y avales de obligaciones, títulos de crédito o instrumentos de deuda a cargo de cualesquiera personas, sociedades, asociaciones e instituciones, de cualquier naturaleza, como quiera que se les denomine y regidas por cualquier legislación, constituyéndose en garante, obligado solidario o mancomunado, fiador o avalista de tales personas.
14. Suscribir, girar, librar, aceptar, endosar y avalar toda clase de títulos de crédito o instrumentos de deuda y llevar a cabo operaciones de crédito y operaciones financieras derivadas, de cualquier naturaleza y regidas por cualquier legislación.
15. Realizar, supervisar o contratar, por cuenta propia o de terceros, toda clase de construcciones, edificaciones o instalaciones para oficinas o establecimientos de cualquier índole.
16. Llevar a cabo, por cuenta propia o de terceros, programas de capacitación y desarrollo, así como trabajos de investigación.
17. Dar o tomar en arrendamiento o en comodato, así como adquirir, poseer, permutar, enajenar, transmitir, disponer o gravar, la propiedad o posesión de toda clase de bienes muebles e inmuebles, incluyendo cualesquiera derechos reales o personales sobre ellos, que sean necesarios o convenientes para su objeto social, independientemente de la legislación que rija tales operaciones o de cómo se les denomine.
18. Actuar como comisionista, mediador, representante o intermediario de cualquier persona física o moral.
19. La producción, transformación, adaptación, comercialización, importación, exportación, compraventa o disposición, conforme a cualquier título legal, de maquinaria, refacciones, materiales, materias primas, productos industriales, efectos y mercaderías de todas clases.
20. Colocar sus propias acciones, valores que las representen, títulos de crédito o instrumentos de deuda, en mercados de valores nacionales o extranjeros, previa autorización de las autoridades competentes cuando sea necesario, incluyendo a través de bolsas de valores o sistemas de cotización extranjeros, solicitar la inscripción de sus valores ante cualquier autoridad de valores nacional o extranjera e inscribir para cotización sus valores en cualquier bolsa de valores o sistema de cotización.
21. Ser agente, comisionista o representante de empresas nacionales o extranjeras.
22. Actuar como comisionista o representante de otras empresas dedicadas a los fines similares.

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

RFC de los integrantes del Consortio:

Participante A: CAS121106653

Participante B: SLA200123919

Participante C: B5T210323521

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

23. La prestación de toda clase de servicios profesionales por cuenta propia o de terceros a personas físicas o en materia de administración, dirección, gerencia, contabilidad, recursos humanos, desarrollo de negocios, asistencia técnica, ejecución de proyectos, asesoría, consultoría, y capacitación, estrategias de ventas y demás servicios profesionales análogos o semejantes a los anteriores, practicar toda clase de estudios de carácter administrativo, diseñar e implantar toda clase de sistemas para la organización o reorganización administrativa, jurídica y/o contable de empresas o instituciones, así como realizar estudios profesionales y técnicos, incluyendo los aspectos jurídicos, corporativos, técnicos, contables, administrativos, financieros, fiscales, informática, mercadotecnia, publicidad, promoción, comercialización, distribución, importación, exportación, fabricación, compra, venta, proyectos y planeación, selección, capacitación y adiestramiento de personal. En general la prestación de toda clase de servicios y su tercerización, A toda clase de personas físicas o morales y negociaciones, instituciones y entidades tanto nacionales como extranjeras.
24. La prestación de servicios profesionales para el desarrollo de toda clase de negocios y/o proyectos, por cuenta propia o de terceros, nacionales o extranjeros a cambio de una contraprestación, así como la celebración de los contratos o convenios necesarios para su realización.
25. La prestación de servicios de toda índole.
26. Emitir acciones no suscritas, para su colocación entre el público.
27. Celebrar fideicomisos y hacer que se emitan certificados de participación ordinarios que representen sus acciones, teniendo o no los mismos el carácter de instrumentos de inversión neutra.
28. Adquirir sus propias acciones, en los términos de la Ley del Mercado de Valores y de las disposiciones de carácter general que sean aplicables.
29. Realizar cualquier acto o designar cualquier comité que fuere requerido o permitido conforme a la legislación aplicable.
30. Adquirir poseer por cualquier título, usar, dar, o tomar en arrendamiento, administrar, vender, enajenar, o disponer en cualquier forma, toda clase de bienes, muebles o inmuebles, así como derechos reales o personales sobre ellos, que sean necesarios o convenientes para la realización de su objeto social.
31. En general realizar todos los actos y operaciones conexos, accesorios o accidentales, que sean necesarios o convenientes para la realización de los objetos anteriores y celebrar todo tipo de contratos y convenios con terceros, incluyendo con accionistas de la Sociedad, en los cuales se establezcan derechos y obligaciones a cargo de la Sociedad, conforme a cualquier legislación que considere conveniente.

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

POR LO QUE CUENTA CON LOS RECURSOS FINANCIEROS, TÉCNICOS, ADMINISTRATIVOS Y HUMANOS PARA OBLIGARSE, EN LOS TÉRMINOS Y CONDICIONES QUE SE ESTIPULAN EN EL PRESENTE CONVENIO.

4.1. "Las Partes" DECLARAN QUE:

4.1.1. CONOCEN LOS REQUISITOS Y CONDICIONES ESTIPULADAS EN LA CONVOCATORIA A LA LICITACIÓN PÚBLICA NACIONAL LA-050GYR019-E182-2022.

4.1.2. MANIFIESTAN SU CONFORMIDAD EN FORMALIZAR EL PRESENTE CONVENIO, CON EL OBJETO DE PARTICIPAR CONJUNTAMENTE EN LA LICITACIÓN, PRESENTANDO PROPUESTA TÉCNICA Y

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx;

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

ECONÓMICA, CUMPLIENDO CON LO ESTABLECIDO EN LA CONVOCATORIA DE LA LICITACIÓN Y CON LO DISPUESTO EN LOS ARTÍCULOS 34, DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO Y 44 DE SU REGLAMENTO.

4.1.3. SEÑALAN COMO DOMICILIO LEGAL PARA TODOS LOS EFECTOS QUE DERIVEN DEL PRESENTE CONVENIO, EL UBICADO EN RIO RHIN NO. 22 INTERIOR 504, COLONIA CUAUHTÉMOC, C.P. 06500 ALCALDÍA CUAUHTÉMOC, CIUDAD DE MÉXICO.

EXPUESTO LO ANTERIOR, LAS PARTES OTORGAN LAS SIGUIENTES.

REC de los integrantes del Consorcio:
Participante A: CAS121106653
Participante B: SJA2001239H9
Participante C: B572103235Z1

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx;

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653

ANEXOS



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022
CLÁUSULAS

PRIMERA.- OBJETO: "PROPOSICIÓN CONJUNTA".

"Las Partes" CONVIENEN, EN CONJUNTAR SUS RECURSOS TÉCNICOS, LEGALES, ADMINISTRATIVOS, ECONÓMICOS Y FINANCIEROS PARA PRESENTAR PROPUESTA TÉCNICA Y ECONÓMICA EN LA LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-050GYR019-E182-2022 Y EN CASO DE SER ADJUDICATARIO DEL CONTRATO, SE OBLIGAN A OTORGAR EL SERVICIO CONTRATADO OBJETO DEL CONVENIO, CON LA PARTICIPACIÓN SIGUIENTE.

CONCEPTO	PARTICIPANTE		
	A	B	C
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.	X		
Clasificador Único de las Contrataciones Públicas (CUCOP): 31900004 Servicios a centros de datos (hospedaje, electricidad, video vigilancia, monitoreo, aire acondicionado, servidores y otros).	CONOCIMIENTO		
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.	CONOCIMIENTO		
1.2. Objetivos Específicos			
<ul style="list-style-type: none"> ▪ 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. 	CONOCIMIENTO		
2. Alcance			
El alcance del SASI 2022-2024 incluye:			

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA2001239H9
 Participante C: BST2103235Z1



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO	PARTICIPANTE		
	A	B	C
<ul style="list-style-type: none"> 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 sustitución, 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. 		X	
<ul style="list-style-type: none"> 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. 		X	
<ul style="list-style-type: none"> 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. 		X	
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:			
<ul style="list-style-type: none"> 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. 			
<ul style="list-style-type: none"> 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. 			CONOCIMIENTO
<ul style="list-style-type: none"> 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. 			
<ul style="list-style-type: none"> 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. 			
<ul style="list-style-type: none"> 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 <i>software</i> y <i>hardware</i> 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 funcionalidades 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 <i>software</i> y <i>hardware</i> 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.			CONOCIMIENTO
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".			

RFC de los integrantes del Consorcio:
Participante A: CAS121106653
Participante B: SLA2001239H9
Participante C: B572103235Z1

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653

ANEXOS
DIVISIÓN DE CONTRATOS



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO	PARTICIPANTE		
	A	B	C
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 (<i>software</i>) 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 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:	X	X	X
Partida 2			
1. Análisis de Vulnerabilidades Estático			
El instituto requiere la continuidad de servicios de análisis de vulnerabilidades estáticos (aseguramiento de aplicaciones) 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 el desarrollo de aplicaciones en sus diferentes etapas de construcción.		X	X
2. Análisis de Vulnerabilidades Dinámico			
El instituto requiere la continuidad de servicios de análisis de vulnerabilidades 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.		X	X
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.		X	X
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.		X	X
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 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.		X	X
<ul style="list-style-type: none"> 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. 		X	X
<ul style="list-style-type: none"> 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. 		X	X
<ul style="list-style-type: none"> Renovación del licenciamiento del <i>software</i> que permite continuar con los servicios y activos de infraestructura que correspondan. 		X	X

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SUAZ001239H9
 Participante C: B572103735Z1

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO	PARTICIPANTE		
	A	B	C
<ul style="list-style-type: none"> 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. 		X	X
<ul style="list-style-type: none"> Identificar los servicios a analizar, incluyendo el número de equipos involucrados y la versión de las plataformas de los sistemas. 		X	X
<ul style="list-style-type: none"> Identificación de vulnerabilidades documentadas en organismos internacionales como el CVE (Common Vulnerability Exposures). 		X	X
<ul style="list-style-type: none"> Identificación de configuraciones por omisión. 		X	X
<ul style="list-style-type: none"> Capacidad para determinar el grado de vulnerabilidad ante técnicas de ataque como: <ul style="list-style-type: none"> - SQL injection - Cross Site Scripting - Cross Site Request Forgery - Sensitive Data Exposure - Security Misconfiguration - Broken Authentication and Session Management 		X	X
<ul style="list-style-type: none"> 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. 		X	X
<ul style="list-style-type: none"> Integrar un proceso y/o procedimiento para la continuidad de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada. 		X	X
<ul style="list-style-type: none"> 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 <i>software</i> descubiertas. 		X	X
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 <i>software</i> con las que cuenta el Instituto, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.		X	X
<ul style="list-style-type: none"> 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. 		X	X
<ul style="list-style-type: none"> Integrar el licenciamiento del <i>software</i> que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios. 		X	X
<ul style="list-style-type: none"> 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 cuenta el servicio correspondiente. 		X	X
<ul style="list-style-type: none"> Integrar un proceso de evaluación de las prácticas existentes de seguridad de <i>software</i> en el Instituto. 		X	X
<ul style="list-style-type: none"> Construir un programa de evaluación de seguridad de <i>software</i> con iteraciones definidas en conjunto con el Instituto. 		X	X
<ul style="list-style-type: none"> Actualizar y crear procesos en las diferentes etapas del ciclo de vida de desarrollo de <i>software</i> para asegurar el mismo. 		X	X
<ul style="list-style-type: none"> Ayudar en el cumplimiento del <i>software</i> basado en estándares y/o marcos normativos previamente definidos en conjunto con el Instituto. 		X	X
<ul style="list-style-type: none"> Identificar el nivel inicial de madurez de las prácticas de seguridad en el <i>software</i> con las que cuenta el Instituto. 		X	X
<ul style="list-style-type: none"> 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. 		X	X
<ul style="list-style-type: none"> Integrar las mejores prácticas de seguridad en el <i>software</i> mencionadas en el modelo de madurez propuesto y alineado a OpenSAMM. 		X	X
<ul style="list-style-type: none"> Realizará la transferencia de las prácticas de seguridad en el <i>software</i> implementadas al personal que el Instituto designe para dicho propósito. 		X	X
<ul style="list-style-type: none"> Operar el modelo de madurez establecido, pudiendo certificar en 3 diferentes etapas el nivel de cumplimiento el <i>software</i> evaluado, las cuales podrán ser: <ul style="list-style-type: none"> - Al inicio del desarrollo de una aplicativo. - Durante el desarrollo de un aplicativo. - Posterior al desarrollo de un aplicativo. 		X	X
<ul style="list-style-type: none"> Preservar la integridad y confidencialidad de la información recibida durante la ejecución de las pruebas dinámicas y/o estáticas correspondientes (cadena de custodia). 		X	X



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO	PARTICIPANTE		
	A	B	C
<ul style="list-style-type: none"> 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. 		X	X
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.		X	X
<ul style="list-style-type: none"> 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. 		X	X
<ul style="list-style-type: none"> 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. 		X	X
<ul style="list-style-type: none"> Identificación de vulnerabilidades y malas configuraciones. 		X	X
<ul style="list-style-type: none"> Explotación de acceso a los sistemas mediante el aprovechamiento de los huecos de seguridad detectados y/o vulnerabilidades detectadas. 		X	X
<ul style="list-style-type: none"> Evaluación de vulnerabilidades de al menos los siguientes rubros: <ul style="list-style-type: none"> - Autenticación y Autorización <ul style="list-style-type: none"> Intentos ilimitados de inicio de sesión Insuficiente autenticación Insuficiente autorización - Gestión de sesión <ul style="list-style-type: none"> Predicción de sesión Secuestro de sesión Reproducir sesión Expiración de sesión insuficiente - Inyección de código <ul style="list-style-type: none"> Inyección comando de Sistema Operativo Inyección SQL Cross-site Scripting Inyección LDAP Inyección HTML Parameters Tampering Cookie Poisoning Hidden Field Manipulation - Criptografía <ul style="list-style-type: none"> Fortaleza del algoritmo Gestión de llaves - Ataques Lógicos <ul style="list-style-type: none"> Abuso de funcionalidades Input Field Validation Checking - Protección de Datos <ul style="list-style-type: none"> Transporte Almacenamiento - Divulgación de Información <ul style="list-style-type: none"> Indexado de directorio Path Traversal Manejo inseguro de errores Comentarios HTML 		X	X
<ul style="list-style-type: none"> 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. 		X	X

RFC de los integrantes del Consorcio:
 Participante A: CAS121106663
 Participante B: SLA200123919
 Participante C: B57210323521



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO	PARTICIPANTE		
	A	B	C
<ul style="list-style-type: none"> Integrar un proceso y/o procedimiento para la continuidad de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada. 		X	X
<ul style="list-style-type: none"> 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. 		X	X
6.2.14. Servicios de Análisis Forense			
<p>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.</p> <ul style="list-style-type: none"> 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 dominan el lenguaje técnico. 		X	X
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.		X	
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.		X	
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 <i>hardware</i> y <i>software</i> necesarios para la incorporación de las soluciones propuestas por el licitante ganador a la red del Instituto, será a cargo del licitante adjudicado.		X	
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.		X	
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.		X	

RFC de los integrantes del Consortio:
 Participante A: CAS121106653
 Participante B: SLA2001239H9
 Participante C: B572103235Z1

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx;

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653

ANEXOS
 DIVISIÓN DE CONTRATOS



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO	PARTICIPANTE		
	A	B	C
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:		X	
<ul style="list-style-type: none"> ▪ 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. 		X	
<ul style="list-style-type: none"> ▪ 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. 		X	
<ul style="list-style-type: none"> ▪ 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). 		X	
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.	X	X	X
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 mesas 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.		X	X
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.		X	X
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.		X	X
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.		X	X
<ul style="list-style-type: none"> • Generar reportes de estado de salud y proponer mejoras y/o soluciones arquitectónicas de la infraestructura de red y seguridad. 		X	X
<ul style="list-style-type: none"> • 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. 		X	X
<ul style="list-style-type: none"> • Desarrollo de recomendaciones de optimización de anchos de banda, mejores rutas, optimización de la infraestructura. 		X	X
<ul style="list-style-type: none"> • Diseño de mejoras sobre la infraestructura y recomendaciones que brinden el más alto desempeño y nivel de servicio. 		X	X
<ul style="list-style-type: none"> • Entrega de reportes proactivos de recomendaciones de actualizaciones de software de los componentes habilitadores que conforman el contrato SASI 2022-2024. 		X	X
<ul style="list-style-type: none"> • Entrega de reporte de análisis detallado del comportamiento de la red de comunicaciones y elementos de seguridad que conforman el contrato SASI 2022-2024. 		X	X

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SJAZ001239H9
 Participante C: BST2103235Z1



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO	PARTICIPANTE						
	A	B	C				
<ul style="list-style-type: none"> 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. 		X	X				
<ul style="list-style-type: none"> Consultoría y recomendaciones de arquitectura de Centro de Datos en base a sus mejores prácticas, dimensionamiento, uso adecuado de recursos. 		X	X				
<ul style="list-style-type: none"> Revisión de los requerimientos de diseño, prioridades y objetivos de acuerdo a lo especificado por el administrador del contrato. 		X	X				
<ul style="list-style-type: none"> Revisión de la arquitectura y topología de la infraestructura de la red. 		X	X				
<ul style="list-style-type: none"> Revisión de la configuración de protocolos. 		X	X				
<ul style="list-style-type: none"> Revisión de la configuración de características de los servicios. 		X	X				
<ul style="list-style-type: none"> Revisión de las mejores practicas en materia de seguridad informática. 		X	X				
<ul style="list-style-type: none"> Recomendación y diseños que permitan incrementar de manera notable las funcionalidades y que conforman la infraestructura tecnológica del Instituto. 		X	X				
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.	X	X	X				
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:		X	X				
<ul style="list-style-type: none"> 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. 		X	X				
<ul style="list-style-type: none"> 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. 		X	X				
<ul style="list-style-type: none"> 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". 		X	X				
<ul style="list-style-type: none"> Incluir la estructura del grupo de trabajo, indicando por cada perfil las responsabilidades y competencias. 		X	X				
El currículo vitae de todo el personal que participe en el servicio, se acreditará 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.		X	X				
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.		X	X				
A continuación, se listan las credenciales y capacidades que deberán cubrir los recursos asignados al proyecto:			X				
Partida 2							
Perfil	Certificaciones a demostrar	Experiencia a demostrar	Función	Número de recursos			
Líder de proyecto	Se deberá presentar alguna las siguientes certificaciones vigentes: PMP (Project Manager Professional) Certificado por PMI ITIL v4 (Expert o Master) 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		X	X

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA2001239H9
 Participante C: BST2103355Z1



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO					PARTICIPANTE		
					A	B	C
Analista de Seguridad	Se deberá presentar la siguiente certificación vigente: 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			
Consultor de Penetración	Se deberá presentar alguna las siguientes certificaciones vigentes: GPEN (GIAC Certified Penetration Tester) 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 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: EnCE (EnCase Certified Examiner) 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. 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.					X	X	X
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.					X	X	
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 (<i>Operational Level Agreement, OLA</i>)	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		X	X	
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				

RFC de los integrantes del Consortio:
Participante A: CAS121106653
Participante B: SLA200123919
Participante C: BST210923521



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO				PARTICIPANTE		
				A	B	C
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:					X	
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 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	Evento	7 días hábiles posteriores a la solicitud generada por parte del Instituto			
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 para el proceso de análisis	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto	X	X	
Servicios de Análisis Forense	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectados 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	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto			

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA2001239H9
 Participante C: BST2103235Z1

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx;

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653

ANEXOS
 DIVISIÓN DE CONTRATOS



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO				PARTICIPANTE		
				A	B	C
tecnológicas utilizadas para el proceso de análisis						
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:				X	X	
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			
	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido	X	X	
	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, 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 funcionarios que sean designados por el primero mencionado.					X	
8. Niveles de servicio que deberán cumplirse (SLA)						
El objetivo de los Niveles de Servicio consiste en proporcionar al Instituto un mecanismo que permita:						
<ul style="list-style-type: none"> 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.						CONOCIMIENTO
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 Deduciones 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".				X	X	
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.						CONOCIMIENTO
Las penas convencionales se aplicarán conforme a lo estipulado en el documento de "Términos y Condiciones".				X	X	
9. Deduciones						
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.						CONOCIMIENTO
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 aplicará una deductiva conforme los niveles de servicios establecidos,						
Las deducciones se aplicarán conforme a lo estipulado en el documento de "Términos y Condiciones".				X	X	

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA2001239H9
 Participante C: BST2103235Z1



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO	PARTICIPANTE		
	A	B	C
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:	X	X	X
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.	X	X	X
b. El "Licitante" deberá implantar y aceptar en todo momento el uso de controles que permitan establecer "Pistas de Auditoría" para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.	X	X	X
c. Los empleados del "Licitante" con acceso a la información sensible del IMSS, deberán firmar acuerdos de confidencialidad con este.	X	X	X
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.	X	X	X
e. El "Licitante" deberá permitir el acceso a información relacionada con el servicio prestado al IMSS para la realización de auditorías.	X	X	X
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.	X	X	X
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:	X	X	X
• Marco normativo de aplicación general y obligatoria en la Administración Pública Federal.	X	X	X
• Artículo 8, segundo y tercer párrafo, fracción I de la Ley Orgánica de la Administración Pública Federal.	X	X	X
• 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.	X	X	X
• Políticas de Seguridad con base en el Sistema de Gestión de Seguridad de la Información (SGSI) del Instituto.	X	X	X
• Certificados ISO/IEC27001:2013 e ISO/IEC20000-1:2018 vigentes a nombre del licitante participante.	X	X	X
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.	X	X	X
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.	X	X	X
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.	X	X	X
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.	X	X	X
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.	X	X	X
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	X	X	X

RFC de los integrantes del Consorcio:
Participante A: CAS121106653
Participante B: SLA200123919
Participante C: B5T210323521

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX
Tel: 55118702; correo: julio.cruz@callit.com.mx;
Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.
RFC: CAS121106653

ANEXOS
DIVISIÓN DE CONTRATOS



Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

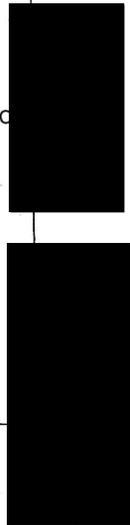
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO	PARTICIPANTE		
	A	B	C
plan deberá permitir 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 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.	X	X	
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.	X	X	
Asimismo, al término del contrato, garantizará los niveles de servicio durante el período de transferencia de servicios al nuevo proveedor.	X	X	
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.	X	X	
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 líderes del proyecto, con apoyo por parte del proveedor del servicio (SOC), garanticen los niveles de servicios establecidos para la operación.			
La estructura organizacional que ejecutará 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.			

CONOCIMIENTO

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA2001239H9
 Participante C: BST2103235Z1



[Firma manuscrita]



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO			PARTICIPANTE		
			A	B	C
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" 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".			
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".			CONOCIMIENTO		
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.			CONOCIMIENTO		
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:					
<ul style="list-style-type: none"> 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 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. 					

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA-200123949
 Participante C: BST210323521

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx;

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653

ANEXOS
DIVISIÓN DE CONTRATOS



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO	PARTICIPANTE		
	A	B	C
5. Normas oficiales o certificaciones			
• Certificado ISO/IEC27001:2013	X		
• Certificado ISO/IEC20000-1:2018	X		
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.	X		
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.	X		
Las modificaciones a las fianzas deberán formalizarse con la participación que corresponda a la afianzadora, en términos de las disposiciones aplicables.	X		
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.	X		
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.	X		
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.	X		
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.	X		
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			

RFC de los integrantes del Consorcio:
Participante A: CAS121106653
Participante B: SLA2001239H9
Participante C: BST2103235Z1



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO				PARTICIPANTE		
				A	B	C
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.				X	X	
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	X	X	
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			
Partida 2						
DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO			
<u>Procedimientos de Operación del servicio</u>						
<ul style="list-style-type: none"> • Servicio de Análisis de Vulnerabilidades Estático • Servicio de Análisis de Vulnerabilidades Dinámico • Servicios de Análisis Forense • 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			
10.3. Servicios del Centro de Operaciones de Seguridad (SOC)						

RFC de los integrantes del Consorcio:
 Participante A: CAS1211066S3
 Participante B: SLA2001239H9
 Participante C: 85T2103235Z1

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX
 Tel: 55118702; correo: julio.cruz@callit.com.mx;
 Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.
 RFC: CAS1211066S3

ANEXOS
DIVISIÓN DE CONTRATOS



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO					PARTICIPANTE		
					A	B	C
10.4. Deducciones					CONOCIMIENTO		
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:							
10.5. Servicios de Seguridad – Verificación/Calidad							
Partida 2							
CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO			
Servicio 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 (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 proceso de análisis	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	X	X	
Servicio 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 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			

RFC de los integrantes del Consortio:
 Participante A: CAS121106653
 Participante B: SLA2001239H9
 Participante C: BST2103235Z1

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx;

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO					PARTICIPANTE		
					A	B	C
herramientas tecnológicas utilizadas para el proceso de análisis							
<u>Servicios de Pruebas de Penetración:</u> 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 para el proceso de análisis	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			
<u>Servicios de Análisis Forense:</u> Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectados 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			
10.6. 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 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 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			

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO					PARTICIPANTE		
					A	B	C
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 realizadas 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 de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento			
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			
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			



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO						PARTICIPANTE		
						A	B	C
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 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 Seguridad (Portal Único)	10 días hábiles posteriores al término de la habilitación de los componentes en los Centros 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				
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.								

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA2001239H9
 Participante C: BS7210323521

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX
 Tel: 55118702; correo: julio.cruz@callit.com.mx;
 Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.
 RFC: CAS121106653

ANEXOS
DIVISIÓN DE CONTRATOS

CONOCIMIENTO



Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO	PARTICIPANTE		
	A	B	C
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:	X		
<ul style="list-style-type: none"> 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-421231-145; que reúna los requisitos fiscales, en la que se indiquen los servicios proporcionados y el número de contrato que ampara dichos servicios, 	X		
<ul style="list-style-type: none"> Original y Copia de la documentación que avale la entrega de los servicios a satisfacción de el instituto (Acta Entrega-Recepción de los Servicios). 	X		
<ul style="list-style-type: none"> 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. 	X		
<ul style="list-style-type: none"> 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. 	X		
<ul style="list-style-type: none"> 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. 	X		
En caso de que el proveedor 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, debiendo presentar nuevamente toda la documentación mencionada anteriormente (en original y/o copia, según corresponda).	CONOCIMIENTO		
El Pago se realizará en pesos mexicanos, en pagos progresivos a mes vencido conforme a las entregas programadas.	X		
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:	X		
12.1. Entregables Generales			
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
			X X

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA2001239H9
 Participante C: B5T2103235Z1

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx;

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO				PARTICIPANTE		
				A	B	C
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			
11						
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:				X	X	
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 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	Evento	7 días hábiles posteriores a la solicitud generada por parte del Instituto		X	X
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	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto			

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA2001239H9
 Participante C: B572103235Z1

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx;

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653

ANEXOS
 DIVISIÓN DE CONTRATOS



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO				PARTICIPANTE		
				A	B	C
	remediación de hallazgos y que incluya 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			
1.1. 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:				CONOCIMIENTO		
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	X	X	
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			
Servicios de Análisis Forense	Reporte que integre el calendario de actualizaciones de versionamiento en <i>software</i> 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.						

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA2001239H9
 Participante C: BST2103235Z1

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX

Tel: 55118702; correo: julio.cruz@callit.com.mx;

Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.

RFC: CAS121106653



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO	PARTICIPANTE		
	A	B	C
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 funcionarios que sean designados por el primero mencionado.	X	X	
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.	X	X	
2. Todos los documentos deben ser entregados en papel membretado de la empresa de manera impresa y en electrónico.	X	X	
3. Se entregará a la División de Seguridad Informática Física perteneciente a la Coordinación de Telecomunicaciones y Seguridad de la Información.	X	X	
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.	X	X	
➤ El horario para la entrega será de las 9:00 horas a las 17:00 horas	X	X	
➤ 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.	X	X	
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:	X	X	X
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.	X	X	X
b. El "Licitante" deberá implantar y aceptar en todo momento el uso de controles que permitan "Pistas de Auditoría" para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.	X	X	X
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.	X	X	X
d. El "Licitante" deberá contar con sistemas que contengan una administración estricta de registros y políticas de retención de la información del IMSS.	X	X	X
e. Los empleados del "Licitante" con acceso a la información sensible del IMSS, deberán firmar acuerdos de confidencialidad con este.	X	X	X
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.	X	X	X
g. El uso de <i>hardware</i> 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.	X	X	X
h. El "Licitante" deberá permitir el acceso a información relacionada con el servicio prestado al IMSS para la realización de auditorías.	X	X	X
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.	X	X	X
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.	X		
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 ponderación establecida en la matriz de evaluación correspondiente.	X	X	X
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.	CONOCIMIENTO		
b) C. Abraham Gutiérrez Castillo, Titular de la División de Seguridad Informática Física.			
c) C. Cynthia Osmary Verdín Villegas, Jefe Área Nivel Central.			

RFC de los integrantes del Consorcio:
 Participante A: CAS121106653
 Participante B: SLA2001229H9
 Participante C: BS7210323521

Rio Rhin No. 22 interior 504, Colonia Cuauhtémoc, C.P. 06500 Alcaldía Cuauhtémoc, CDMX
 Tel: 55118702; correo: julio.cruz@callit.com.mx;
 Razón Social: CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V.
 RFC: CAS121106653

ANEXOS
 DIVISIÓN DE CONTRATOS



SE CANCELAN DATOS PERSONALES DE PERSONA(S) FÍSICA(S) IDENTIFICABLE(S) TALES COMO: NOMBRE Y FIRMA, 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

Consortio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la
Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO	PARTICIPANTE		
	A	B	C
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.	CONOCIMIENTO		
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.	CONOCIMIENTO		
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:	CONOCIMIENTO		
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.	CONOCIMIENTO		
23. Mecanismos requeridos al proveedor para responder por defectos o vicios ocultos de los bienes o de la calidad de los servicios			
No aplica	CONOCIMIENTO		
24. Otorgamiento de anticipo			
No aplica	CONOCIMIENTO		

SEGUNDA.-REPRESENTANTE COMÚN Y OBLIGADO SOLIDARIO.

"Las Partes" ACEPTAN EXPRESAMENTE EN DESIGNAR COMO REPRESENTANTE COMÚN AL "PARTICIPANTE A" A TRAVÉS DEL PRESENTE INSTRUMENTO, OTORGÁNDOLE PODER AMPLIO Y SUFICIENTE, PARA ATENDER TODO LO RELACIONADO CON LAS PROPUESTAS TÉCNICA Y ECONÓMICA EN EL PROCEDIMIENTO DE LICITACIÓN, ASÍ COMO PARA SUSCRIBIR DICHAS PROPUESTAS.

ADICIONALMENTE, "Las Partes" ACUERDAN QUE EL "PARTICIPANTE A" SERÁ RESPONSABLE DE REALIZAR TODAS LAS GESTIONES ADMINISTRATIVAS DURANTE LA VIGENCIA DEL CONTRATO, Y QUE SERÁ EL PUNTO DE CONTACTO CON EL ADMINISTRADOR DEL CONTRATO POR PARTE DEL INSTITUTO, YA SEA DE MANERA CONJUNTA CON EL PROJECT MANAGER PROPUESTO PARA LA PRESTACIÓN DEL SERVICIO, O DE FORMA INDEPENDIENTE.

ACUERDAN TAMBIÉN QUE TODO LO NO PREVISTO EN EL PRESENTE CONVENIO, SERÁ ATENDIDO POR EL REPRESENTANTE COMÚN, Y RESUELTO CONFORME A LAS RESPONSABILIDADES QUE A CADA PARTICIPANTE CORRESPONDA.

ASIMISMO, CONVIENEN ENTRE SI EN CONSTITUIRSE EN FORMA CONJUNTA Y SOLIDARIA PARA COMPROMETERSE POR CUALQUIER RESPONSABILIDAD DERIVADA DEL CUMPLIMIENTO DE LAS OBLIGACIONES ESTABLECIDAS EN EL PRESENTE CONVENIO, EN RELACIÓN CON EL CONTRATO QUE SUS REPRESENTANTES LEGALES FIRMAN CON EL INSTITUTO MEXICANO DEL SEGURO SOCIAL (IMSS), DERIVADO DEL PROCEDIMIENTO DE CONTRATACIÓN LA-050GYR019-E182-2022, ACEPTANDO EXPRESAMENTE EN RESPONDER ANTE EL IMSS POR LAS PROPUESTAS QUE SE PRESENTEN Y, EN SU CASO, DE LAS OBLIGACIONES QUE DERIVEN DE LA ADJUDICACIÓN DEL CONTRATO RESPECTIVO.

Consorcio Conformado por CONSULTING ALL SERVICE IN TELECOM AND MEDICE S. DE R.L. DE C.V., BOHMER STRATEGISTS, S. DE R.L. DE C.V. y SECURE LABS, S.A. DE C.V., quienes participan de forma conjunta en la

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

TERCERA.- DEL COBRO DE LAS FACTURAS.

"Las Partes" CONVIENEN EXPRESAMENTE, QUE "EL PARTICIPANTE A", REALIZARÁ EL COBRO DE LAS FACTURAS RELATIVAS AL SERVICIO QUE SE PROPORCIONE AL IMSS, CON MOTIVO DEL CONTRATO QUE SE DERIVE DE LA LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-050GYR019-E182-2022.

CUARTA.- VIGENCIA.

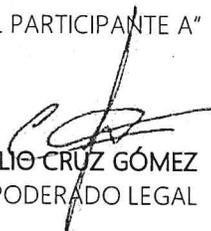
"Las Partes" CONVIENEN, EN QUE LA VIGENCIA DEL PRESENTE CONVENIO SERÁ EL DEL PERÍODO DURANTE EL CUAL SE DESARROLLE EL PROCEDIMIENTO DE LA LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-050GYR019-E182-2022 INCLUYENDO, EN SU CASO, DE RESULTAR ADJUDICADOS DEL CONTRATO, EL PLAZO QUE SE ESTIPULE EN ÉSTE Y EL QUE PUDIERA RESULTAR DE CONVENIOS DE MODIFICACIÓN.

QUINTA.- OBLIGACIONES.

"Las Partes" CONVIENEN EN QUE EN EL SUPUESTO DE QUE CUALQUIERA DE ELLAS QUE SE DECLARE EN QUIEBRA O EN SUSPENSIÓN DE PAGOS, NO LAS LIBERA DE CUMPLIR CON SUS OBLIGACIONES, POR LO QUE CUALQUIERA DE ELLAS QUE SUBSISTA, ACEPTA Y SE OBLIGA EXPRESAMENTE A RESPONDER SOLIDARIAMENTE DE LAS OBLIGACIONES CONTRACTUALES A QUE HUBIERE LUGAR.

LEÍDO QUE FUE EL PRESENTE CONVENIO POR "Las Partes" Y ENTERADOS DE SU ALCANCE Y EFECTOS LEGALES, ACEPTANDO QUE NO EXISTIÓ ERROR, DOLO, VIOLENCIA O MALA FE, LO RATIFICAN Y FIRMAN, DE CONFORMIDAD EN LA CIUDAD DE MÉXICO, EL DÍA 26 DE SEPTIEMBRE DE 2022.

"EL PARTICIPANTE A"


JULIO CRUZ GÓMEZ
APODERADO LEGAL

"EL PARTICIPANTE B"


PRESIDENTE DEL CONSEJO DE
GERENTES

"EL PARTICIPANTE C"


ALBERTO VARGAS MAGAÑA
APODERADO LEGAL

SIN TEXTO