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

Contrato Abierto para la prestación de los Servicios Administrados de Seguridad Informática Continuidad (SASI-C), que celebran por una parte, el **INSTITUTO MEXICANO DEL SEGURO SOCIAL**, que en lo sucesivo se denominará **"EL INSTITUTO"**, representado en este acto por la **C. MARÍA GABRIELA QUINTANAR OLVERA**, en su carácter de Apoderada Legal, y por la otra parte, la empresa denominada **TOTALSEC, S.A. DE C.V.**, a quien en lo sucesivo se le denominará **"EL PROVEEDOR"**, representada por el **C. VÍCTOR RODRÍGUEZ FUENTES**, en su carácter de Representante Legal, y a quienes en forma conjunta se les denominará **"LAS PARTES"**, al tenor de las Declaraciones y Cláusulas siguientes:

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

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

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

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

I.3.- La C. María Gabriela Quintanar Olvera, en su carácter de Titular de la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos, cuenta con las facultades suficientes para suscribir el presente instrumento jurídico en su calidad de Apoderada Legal, de conformidad con lo establecido en los artículos 268 A de la Ley de Seguro Social y 66 último párrafo del Reglamento Interior del Instituto Mexicano del Seguro Social, y acredita su personalidad mediante el testimonio de la Escritura Pública número 77,897 de fecha 16 de junio de 2021, otorgada ante la fe del Licenciado Ignacio Soto Sobreyra y Silva, Titular de la Notaría Pública Número 13 de la Ciudad de México, e inscrita en el Registro Público de Organismos Descentralizados bajo el folio número 97-7-24062021-194125, de fecha 24 de junio de 2021, y manifiesta bajo protesta de decir verdad que las facultades que le fueron conferidas no le han sido revocadas, modificadas, ni restringidas en forma alguna en cumplimiento a los artículos 24 y 25 de la Ley Federal de las Entidades Paraestatales.

I.4.- El C. Abraham Gutiérrez Castillo, Titular de la División de Seguridad Informática Física de **"EL INSTITUTO"**, funge como administrador del presente contrato, responsable de dar seguimiento y verificar el cumplimiento de los derechos y obligaciones establecidos en este instrumento jurídico, de conformidad con lo dispuesto en el artículo 84, penúltimo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

I.5.- Para el cumplimiento de sus funciones y la realización de sus actividades se requiere de la prestación de los Servicios Administrados de Seguridad Informática Continuidad (SASI-C), solicitado por la Coordinación de Telecomunicaciones y Seguridad de la Información.

I.6.- Para cubrir las erogaciones que se deriven del presente contrato, cuenta con los recursos disponibles suficientes, no comprometidos, en la cuenta número 42062493 de conformidad con el Dictamen de Disponibilidad Presupuestal Previo con número de folio 0000031960-2022, emitido por la Titular de la División de Control y Seguimiento al Presupuesto de Operación en Ámbito Central de fecha 21 de febrero de 2022, documento que se agrega en el **Anexo 1 (uno)** del presente contrato.

I.7.- Con fecha 04 de marzo de 2022, la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos, a través de la División de Contratación de Activos y Logística, notificó a **"EL PROVEEDOR"** en el Procedimiento de Adjudicación Directa Nacional número **AA-050GYR019-E22-2022**, con fundamento en lo dispuesto en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos, 26 fracción III, 28 fracción I, 40, 41 fracción V y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, los relativos de su Reglamento y demás disposiciones aplicables en la materia, como se detalla en el **Anexo 2 (dos)**, del presente instrumento jurídico.

I.8.- De conformidad con lo previsto en el artículo 81, fracción IV del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en caso de discrepancia entre el contenido en el Oficio de Solicitud de Cotización y el presente instrumento jurídico, prevalecerá lo establecido en dicha Solicitud.

I.9.- Señala como su domicilio para todos los efectos de este acto jurídico, el ubicado en Calle Durango número 291, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, en la Ciudad de México.

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

II.1.- Es una persona moral constituida de conformidad con las leyes de los Estados Unidos Mexicanos, según consta en la Escritura Pública número 100,395 de fecha 21 de septiembre de 2015, pasada ante la fe del Licenciado Jorge Alfredo Domínguez Martínez, Titular de la Notaría Pública número 140 del Distrito Federal, e inscrita en el Registro Público de la Propiedad y de Comercio del Distrito Federal, en el folio mercantil electrónico número 553823-1.

II.2.- El C. Víctor Rodríguez Fuentes, acredita su personalidad en términos la Escritura Pública número 88,711 de fecha 02 de octubre de 2020, pasada ante la fe del Licenciado Francisco I. Hugues Vélez, Titular de la Notaría Pública número 212, en cuyo protocolo actúan también los Licenciados Rosamaría López Lugo, Titular de la Notaría número 223 y Guillermo Oliver Bucio, Titular de la Notaría número 246, los tres por convenio de sociedad, de la Ciudad de México, e inscrita en el Registro Público de la Propiedad y de Comercio del Distrito Federal, en el folio mercantil electrónico número 553823-1, y manifiesta bajo protesta de decir verdad que las facultades que le fueron conferidas no le han sido revocadas, modificadas ni restringidas en forma alguna.

II.3.- Su objeto social conforme a sus Estatutos consiste, entre otros, en consultoría, diseño, integración e implantación de arquitecturas de seguridad (procesos, personas, tecnología).

II.4.- Cuenta con los registros siguientes:

- Registro Federal de Contribuyentes número: **TOT1509213Y5**.
- Registro Patronal ante **"EL INSTITUTO"** y **EL INFONAVIT** número: [redacted]

II.5.- Cuenta con el documento vigente expedido por el Servicio de Administración Tributaria (SAT), de opinión de cumplimiento de obligaciones fiscales en sentido positivo, de conformidad con el artículo 32 D del Código Fiscal de la Federación, así como a lo dispuesto por las Reglas 2.1.29 y 2.1.37 de la Resolución Miscelánea Fiscal para 2022, publicada el 27 de diciembre de 2021 en el Diario Oficial de la Federación, del cual presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

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

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

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

II.8.- Cuenta con el documento correspondiente vigente, expedido por el INFONAVIT en los términos del Acuerdo del H. Consejo de Administración del Instituto del Fondo Nacional de la Vivienda para los Trabajadores por el que se emiten las Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos, publicado en el Diario Oficial de la Federación el 28 de junio de 2017, del cual presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.

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

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

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

II.10.- Conforme a lo previsto en los artículos 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 107 de su Reglamento, **"EL PROVEEDOR"**, en caso de auditorías, visitas o inspecciones que practique la Secretaría de la Función Pública y el Órgano Interno de Control en **"EL INSTITUTO"** y cualquier otra entidad fiscalizadora, deberá proporcionar la información relativa al presente contrato que en su momento se requiera, generada desde el procedimiento de adjudicación hasta la conclusión de la vigencia, a efecto de ser sujetos a fiscalización de los recursos de carácter federal.

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

II.12.- Para efectos legales y de notificación relacionados con el presente contrato, señala como domicilio para oír y recibir toda clase de notificaciones y documentos, el ubicado en Avenida Periférico Sur número 4121, Colonia Fuentes del Pedregal, Demarcación Territorial Tlalpan, Código Postal 14140, en la Ciudad de México, teléfono: (55) 4509-9858, correos electrónicos: [redacted] y [redacted]

Hechas las declaraciones anteriores, **"LAS PARTES"** convienen en otorgar el presente contrato, de conformidad con las siguientes:

C L Á U S U L A S

PRIMERA.- OBJETO DEL CONTRATO.- "EL PROVEEDOR" se obliga a prestar los Servicios Administrados de Seguridad Informática Continuidad (SASI-C), cuyas características, cantidades, alcances y especificaciones se describen en los **Anexos 1 (uno)** y **2 (dos)** del presente instrumento jurídico, así como a las condiciones de la solicitud de cotización y oficio de notificación de adjudicación.

SEGUNDA.- IMPORTE DEL CONTRATO.- El importe del presente contrato es por la cantidad mínima de **$53,626,097.00 (CINCUENTA Y TRES MILLONES SEISCIENTOS VEINTISÉIS MIL NOVENTA Y SIETE PESOS 00/100 M.N.)**, más el Impuesto al Valor Agregado (I.V.A.), y por la cantidad máxima de **$59,586,168.00 (CINCUENTA Y NUEVE MILLONES QUINIENTOS OCHENTA Y SEIS MIL CIENTO SESENTA Y OCHO PESOS 00/100 M.N.)**, más el Impuesto al Valor Agregado (I.V.A.), de conformidad con los precios unitarios que se indican en el **Anexo 2 (dos)** del presente contrato.

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

TERCERA.- FORMA Y CONDICIONES DE PAGO.- Se efectuarán pagos a **"EL PROVEEDOR"** una vez prestado el servicio, de conformidad con lo dispuesto en los artículos 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 93 de su Reglamento, así como

por lo establecido en los Términos y Condiciones que se agregan al presente contrato en el **Anexo 1 (uno)**.

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, será el responsable de recibir y aceptar cada uno de "Los Servicios", así como realizará los trámites de pago en cumplimiento al procedimiento administrativos vigente en **"EL INSTITUTO"**.

Para proceder a la liberación de pago, el Titular 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 contractuales a cargo de **"EL PROVEEDOR"**, así como de la ejecución, validación, técnica y administrativa de todos y cada uno de los documentos que acreditan que los servicios proporcionados por **"EL PROVEEDOR"** se cumplieron en tiempo, forma y cantidad y que cumplen con las características, especificaciones y condiciones requeridas, procederá el pago de conformidad con lo establecido en el artículo 51 de la LAASSP.

"EL PROVEEDOR" deberá entregar en la División de Trámite de Erogaciones, situada en la calle de Tiburcio Montiel No. 15, PB, Col. San Miguel Chapultepec, Código Postal 11850, Demarcación Territorial Miguel Hidalgo, Ciudad de México, 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, Demarcación Territorial Cuauhtémoc, C.P. 06600, Ciudad de México, 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 aplicará la ejecución de garantía.

El pago se realizará en pesos mexicanos, en los plazos normados por la Dirección de Finanzas en el "Procedimiento para la recepción, glosa y aprobación de documentos presentados para

trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos", sin que éstos rebasen los 20 (veinte) días naturales posteriores a aquel en que **"EL PROVEEDOR"** presente en las áreas de trámite de erogaciones la representación impresa del Comprobante Fiscal Digital por Internet (CFDI).

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

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

Para la validación de dichos comprobantes **"EL PROVEEDOR"** deberá cargar en internet, a través del portal de servicios a proveedores de la página de **"EL INSTITUTO"** el archivo en formato XML, la validez de los mismos será determinada durante la carga y únicamente los comprobantes válidos serán procedentes para pago.

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

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

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

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

"EL PROVEEDOR" se obliga a no cancelar ante el SAT los CFDI a favor de **"EL INSTITUTO"** previamente validados en el portal de servicios a proveedores, salvo justificación y

comunicación por parte del mismo al administrador del contrato para su autorización expresa, debiendo éste informar a las áreas de trámite de erogaciones de dicha justificación y reposición del CFDI en su caso.

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

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

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

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

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

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

En caso de que **"EL PROVEEDOR"** reciba pagos en exceso deberá reintegrar las cantidades pagadas en exceso más los intereses correspondientes, conforme a la tasa que establezca la Ley de Ingresos de la Federación, en los casos de prórroga para el pago de créditos fiscales. Los intereses se calcularán sobre las cantidades en exceso y se computarán por días naturales desde la fecha de su entrega hasta la fecha en que se pongan efectivamente las cantidades a disposición de **"EL INSTITUTO"**.

En caso de que **"EL PROVEEDOR"** presente su CFDI con errores o deficiencias, conforme a lo previsto en los artículos 89 y 90 del Reglamento de la Ley de Adquisiciones, Arrendamientos y

Servicios del Sector Público, **"EL INSTITUTO"** dentro de los 3 (tres) días hábiles siguientes a la recepción de la misma, indicará por escrito a **"EL PROVEEDOR"** las deficiencias o errores que deberá corregir. El periodo que transcurra a partir de la entrega del citado escrito y hasta que **"EL PROVEEDOR"** presente las correcciones no se computará dentro del plazo estipulado para el pago.

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

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

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

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

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

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

PLAZO DE LA PRESTACIÓN DEL SERVICIO.- El servicio iniciará a partir del día hábil siguiente al de la notificación de la adjudicación y hasta el 31 de agosto de 2022.

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

Asimismo, **"EL PROVEEDOR"** se obliga a cumplir con los plazos y actividades señalados en el Anexo Técnico y los Términos y Condiciones integrados en el **Anexo 1 (uno)** del presente contrato.

LUGAR DE LA PRESTACIÓN DEL SERVICIO.- "EL PROVEEDOR" se obliga a prestar el servicio de conformidad con lo siguiente:

- 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, Demarcación Territorial Cuauhtémoc, C.P. 06600, en la Ciudad de México.
- 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, Demarcación Territorial Cuauhtémoc, C.P. 06600, en la Ciudad de México.

Lo anterior, conforme a lo señalado en el numeral 13 de los Términos y Condiciones que se Agregan en el **Anexo 1 (uno)** del presente contrato.

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

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

QUINTA.- VIGENCIA.- "LAS PARTES" convienen que la vigencia del presente contrato será a partir del día hábil siguiente a la notificación de la adjudicación y hasta el 31 de agosto de 2022.

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

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

Si con motivo de la transferencia de los derechos de cobro solicitada por **"EL PROVEEDOR"** se origina un retraso en el pago, no procederá el pago de los gastos financieros a que hace

referencia el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

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

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

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

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

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

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

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

En caso de que sobreviniera alguna reclamación en contra de **"EL INSTITUTO"** por cualquiera de las causas antes mencionadas, la única obligación de éste será la de dar aviso en el domicilio previsto en este instrumento jurídico a **"EL PROVEEDOR"**, para que éste lleve a cabo las acciones necesarias que garanticen la liberación de **"EL INSTITUTO"** de cualquier

controversia o responsabilidad de carácter civil, mercantil, penal o administrativa que, en su caso, se ocasione.

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

Asimismo, **"EL PROVEEDOR"** se obliga a cumplir con lo señalado en el numeral 15 de los Términos y Condiciones que se agregan en el **Anexo 1 (uno)** del presente contrato.

DÉCIMA.- GARANTÍA.- "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 del artículo 81, fracción VI del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y de la Ley de Instituciones de Seguros y de Fianzas a favor del "Instituto Mexicano del Seguro Social" por un monto equivalente al 10% (diez por ciento) sobre el importe máximo que se indica en la Cláusula Segunda del presente contrato, sin considerar el Impuesto al Valor Agregado (I.V.A.), en Moneda Nacional.

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

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

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

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

a) Se rescinda administrativamente el presente contrato.

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

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

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

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

DÉCIMA SEGUNDA.- PENAS CONVENCIONALES.- De conformidad con lo establecido en los artículos 45, fracción XIX, 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 95 y 96 de su Reglamento, la pena convencional aplicable a **"EL PROVEEDOR"**, por atraso en el cumplimiento de la prestación del servicio será conforme a los conceptos y porcentajes señalados en los numerales 9.1, 9.2, 9.3, 9.4 y 9.5 de los Términos y Condiciones incluidos en el **Anexo 1 (uno)** del presente contrato.

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

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

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

DÉCIMA TERCERA.- DEDUCCIONES.- Con fundamento en lo dispuesto en los artículos 53 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 97 de su Reglamento, **"EL PROVEEDOR"**, por la entrega parcial o deficiente del servicio, se hará acreedor a una sanción conforme los conceptos y porcentajes señalados en los numerales 9.6, 9.7, 9.8, 9.9, 9.10, 9.11, 9.12, 9.13 y 9.14 de los Términos y Condiciones que se integran en el **Anexo 1 (uno)** del presente contrato.

El administrador del presente contrato será responsable del cálculo, aplicación y seguimiento de las deducciones. El monto máximo de aplicación de las deducciones no podrán ser mayor al que resulte de aplicar el porcentaje de la garantía de cumplimiento del presente contrato.

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

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

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

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

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

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

1. Cuando no entregue la garantía de cumplimiento del presente contrato, a más tardar dentro de los 10 (diez) días naturales posteriores a la firma del mismo.

2. Cuando incurra en falta de veracidad total o parcial respecto a la información proporcionada para la celebración del presente contrato.
3. Cuando se compruebe que el servicio ha sido prestado con alcances y características distintas a las pactadas.
4. Cuando se transmitan total o parcialmente, bajo cualquier título y a favor de otra persona física o moral, los derechos y obligaciones a que se refiere el presente documento, con excepción de los derechos de cobro, previa autorización de **"EL INSTITUTO"**.
5. Si la autoridad competente declara el concurso mercantil o cualquier situación análoga o equivalente que afecte el patrimonio de **"EL PROVEEDOR"**.
6. Cuando de manera reiterativa y constante, **"EL PROVEEDOR"** sea sancionado por parte de **"EL INSTITUTO"** con penalizaciones y/o deducciones sobre el mismo concepto de los servicios que proporciona, o por ubicarse en los límites de incumplimientos previstos en la cláusula de penas convencionales y/o deducciones del presente instrumento.
7. Cuando se sitúe en alguno de los supuestos previstos en el artículo 50 de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público.
8. Si **"EL PROVEEDOR"** no permite a **"EL INSTITUTO"** la administración y verificación a que se refiere la cláusula correspondiente del presente contrato.
9. Cuando incumpla, total o parcialmente, con cualesquiera de las obligaciones establecidas en el presente contrato y sus anexos.

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

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

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

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

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

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

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

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

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

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

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

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

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

DÉCIMA NOVENA.- CONFIDENCIALIDAD.- "EL PROVEEDOR" de los Servicios Administrados de Seguridad Informática Continuidad (SASI-C), deberá suscribir con el Administrador del presente contrato, el Convenio de Confidencialidad y Resguardo de Información correspondiente, en el que su representada o cualquiera de su personal asignado al proyecto por ningún motivo extraerán o divulgará el contenido de la información que se les entregará como parte del presente contrato.

Dicho documento debe ir firmado por su representante legal, en la que manifieste, que se compromete a respetar y seguir los estándares tecnológicos, tanto de metodologías, procedimientos, hardware, como de software definidos por **"EL INSTITUTO"**.

Asimismo, en dicha carta **"EL PROVEEDOR"** deberá indicar que se compromete a que toda la información que exista a la fecha de la adjudicación y aquella que desarrolle derivado del presente proyecto será propiedad intelectual y exclusiva de **"EL INSTITUTO"** y no podrá ser utilizada por **"EL PROVEEDOR"** para otros fines.

Por lo que deberá considerar al menos los siguientes mecanismos de control de acceso a la información de **"EL INSTITUTO"**:

- Se deberán establecer controles de acceso y privilegios restringidos al personal del Proveedor del SASI-C, a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones de **"EL INSTITUTO"**.
- Se deberá implantar y aceptar en todo momento el uso de controles que permitan registrar "Pistas de Auditoria" para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.
- La seguridad lógica deberá estar protegida mediante el uso de dispositivos de control de acceso (Firewalls), mecanismos de encriptación y seguridad física entre las redes del Proveedor del SASI-C y las de **"EL INSTITUTO"**.
- El almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por **"EL PROVEEDOR"** de los servicios SASI-C, observando los requisitos de seguridad y resguardo de la información.
- **"EL PROVEEDOR"** del SASI-C deberá permitir el acceso a información relacionada con el servicio prestado a **"EL INSTITUTO"** para la realización de auditorías.
- **"EL PROVEEDOR"** SASI-C 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.

VIGÉSIMA.- MODIFICACIONES.- De conformidad con lo establecido en el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"EL INSTITUTO"** podrá celebrar por escrito Convenio Modificatorio, al presente contrato dentro de la vigencia del

mismo. Para tal efecto, **"EL PROVEEDOR"** se obliga a entregar, en su caso, la modificación de la garantía, en términos del artículo 103, fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

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

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

VIGÉSIMA PRIMERA.- ADMINISTRACIÓN Y VERIFICACIÓN.- El C. Abraham Gutiérrez Castillo, Titular de la División de Seguridad Informática Física de **"EL INSTITUTO"**, funge como administrador del contrato, responsable de administrar y verificar su cumplimiento, de conformidad con lo establecido en el documento de designación de administrador del contrato que se agrega al presente como **Anexo 3 (tres)** y el artículo 84 penúltimo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

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

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

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

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

VIGÉSIMA CUARTA.- LEGISLACIÓN APLICABLE.- "LAS PARTES" se obligan a sujetarse estrictamente para el cumplimiento del presente contrato, a todas y cada una de las cláusulas

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

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

del mismo, así como a lo establecido en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento y supletoriamente al Código Civil Federal, a la Ley Federal de Procedimiento Administrativo, al Código Federal de Procedimientos Civiles y demás ordenamientos aplicables en la materia.

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

Previa lectura y debidamente enteradas **"LAS PARTES"** del contenido, alcance y fuerza legal del presente contrato, en virtud de que se ajusta a la expresión de su libre voluntad y que su consentimiento no se encuentra afectado por dolo, error, mala fe, ni otros vicios de la voluntad, lo firman y ratifican en todas sus partes, por triplicado, en la Ciudad de México, el **18 de marzo 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

C. MARÍA GABRIELA QUINTANAR OLVERA
Apoderada Legal

POR "EL PROVEEDOR"
TOTALSEC, S.A. DE C.V.

C. VÍCTOR RODRÍGUEZ FUENTES
Representante Legal

ADMINISTRADOR DEL CONTRATO

C. ABRAHAM GUTIÉRREZ CASTILLO
Titular de la División de Seguridad Informática Física

RRSR/HRJ/JMHN/RMVS.

IMSS	INSTITUTO MEXICANO DEL SEGURO SOCIAL DIRECCIÓN DE ADMINISTRACIÓN UNIDAD DE ADQUISICIONES COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS	Contrato Número S2M0038

ANEXO 1 (UNO)

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

EL PRESENTE ANEXO CONSTA DE **52** HOJAS INCLUYENDO ESTA CARÁTULA

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: 0000031960-2022

[ ] Dictamen de Inversión
[X] Dictamen de Gasto

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

Concepto: OF. 148 RECIBIDO EL 18/02/2022 "SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMATICA CONTINUIDAD (SASIC)", PARA EL EJERCICIO 2022.

Fecha Elaboración: 21/02/2022

Total Compromiso (en pesos): $ 99,184,154.88
Cuenta: 42002493 Serv Int Infraestructura Compu Unidad de Información: 099001 Centro de Costos: 500000
Partida Presupuestaria SHCP: 31904 Servicios integrales de infraestructura de cómputo

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
	0.0	0.0	0.0	33,061.4	16,530.7	16,530.7	16,530.7	16,530.7	0.0	0.0	0.0	0.0
	0.0	0.0	0.0	85,246.0	176,464.0	76,479.4	53,854.4	110,521.0	0.0	0.0	0.0	0.0

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

ATENTAMENTE

Lic. Jessica Miranda Vega
Titular Div de Ctrl y Seguimiento al Ppto de Oper en Ámbito Central

DIA | MES | AÑO
DICTAMINADO DEFINITIVO

DICTAMEN DEFINITIVO

CONTRATO No.

IMPORTE DEFINITIVO (EN PESOS): $ .00

Clave: 6170-009-001

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

INSTITUTO MEXICANO DEL SEGURO SOCIAL

DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

COORDINACIÓN DE TELECOMUNICACIONES Y SEGURIDAD DE LA INFORMACIÓN

ANEXO TÉCNICO

SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA CONTINUIDAD (SASI-C)

2022

Contenido

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	Septiembre 30 2021	Actualización del Documento	Lic. Cynthia Osmara Verdín Villegas
0.2	Septiembre 30 2021	Revisión del Documento	Ing. Abraham Gutierrez Castillo
1.0	Septiembre 30 2021	Aprobación del Documento	Lic. Florencio Fernando González Velazquez

1. Objetivo

El Instituto Mexicano del Seguro Social (IMSS), actualmente cuenta con un servicio administrado de seguridad integral, que provee la infraestructura de toda la gama de equipos de seguridad con los que se da atención a los servicios y a las aplicaciones propias del IMSS, por lo que con el propósito de mantener la continuidad de la operación del día a día del negocio, es indispensable contar con niveles de servicio de alta disponibilidad que garanticen la operación de la infraestructura de seguridad, almacenamiento, comunicaciones y respaldos, así como otros componentes habilitadores, que soportan los Servicios operativos institucionales, aplicando las mejores prácticas de TI y garantizando los niveles de servicio, calidad y oportunidad solicitados por el IMSS.

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 que garanticen la continuidad operativa, de negocios y de seguridad de la información del Instituto.

2. Beneficios

Los beneficios del Servicio de Seguridad Informática son los siguientes:

- Garantizar la continuidad operativa, la continuidad del negocio y la continuidad de la seguridad de la información en la Institución.
- Fortalecer la seguridad de la información de la Institución contra amenazas, disminuyendo el riesgo de sufrir incidentes de seguridad, mediante el uso de tecnologías de punta para el monitoreo, detección, aseguramiento, y contención de ataques que puedan presentarse en la infraestructura de cómputo, sistemas y aplicaciones propios del IMSS.
- Garantizar la confidencialidad de la información que el IMSS genera, recibe y procesa en su operación.
- Contar con servicios medidos por niveles de servicio, que migren, habiliten y mantengan a punto los componentes necesarios en los centros de datos del Instituto y que de forma complementaria gestionen operen, monitoreen, den soporte y mantenimiento preventivo y correctivo a la infraestructura, con el propósito de satisfacer las necesidades que se tienen en cuanto a conectividad, comunicación, protección, control y filtrado de la propia Institución, manteniendo la plataforma tecnológica en condiciones óptimas de operación.
- Contar con servicios de seguridad de la información, que complementen el esquema de seguridad institucional de forma consistente y robusta, con el control, aseguramiento, diagnóstico, protección, pruebas, metodologías, de distintos rubros como el de acceso a cuentas privilegiadas, base de datos, aplicaciones, fuentes múltiples, vulnerabilidades, investigación forense y de procesos de seguridad, así como con otros servicios especializados en materia de seguridad y tecnologías de la información.
- Contar con servicios de soporte extendido que son necesarios para dar continuidad a los Servicios Administrados de Seguridad Informática Continuidad (SASI-C).
- Contar con personal calificado con la experiencia requerida para soportar todos y cada uno de los requerimientos del Instituto.

3. Alcance

Es establecer las especificaciones y lineamientos técnicos para la prestación del Servicio de Seguridad Informática.

El Instituto requiere de Servicios Administrados de Seguridad Informática Continuidad (SASI-C), con la finalidad de mantener, robustecer y complementar la seguridad institucional, centros de datos propios o de terceros en instalaciones del Instituto, o donde este lo requiera.

El proyecto abarca la toma de operación para las tecnologías funcionales de seguridad con las que cuenta hoy en día el Instituto como son: Firewalls, IPS, Filtrado de Contenido, Anti DDoS, Antispan, WAF, DBF, VPN, UTM, entre otras, la actualización tecnológica en *hardware* y *software* durante el período de transición.

Al término de la vigencia del contrato, el proveedor deberá considerar un periodo de dos meses para la transición a un nuevo proveedor de servicios, que se utilizaran para la entrega de toda la documentación técnica correspondiente al servicio que se encuentre en operación a la conclusión de los servicios y contar con el apoyo en todo momento para la transición.

4. Requerimientos del servicio

Los Servicios requeridos y que deberán ser parte de la solución propuesta deberá incluir al menos lo siguiente:

- **Servicios de Seguridad - Continuidad Operativa**
  Son los servicios de continuidad operativa para la seguridad perimetral que incluye los siguientes: (Firewalls, IPS, AntiDDoS, Filtrado Web, Firewall de Aplicaciones WEB, Firewall de base de datos, cifrado de información, Control de Accesos, entre otros.), servicios que deberán cumplir con los niveles de servicio establecidos para que de manera inmediata y en donde lo requiera el Instituto se continue con la operación. Estos servicios serán bajo demanda conforme a petición expresa del instituto, así como los tiempos de entrega serán conforme al sitio y dependiendo del tipo de tecnología.

- **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, las pruebas de vulnerabilidades (revisiones de vulnerabilidades a los aplicativos y sistemas de información), cumplimiento normativo y herramientas de seguridad, así como los niveles de servicio requeridos la operación, incluyendo el soporte y resolución de problemas e incidentes.

- **Servicios del Centro de Operaciones de Seguridad (SOC)**
  El Instituto requiere que el proveedor del servicio cuente con un Centro de Operaciones de la 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, 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 funcionamiento

7x24x365, etc.) El SOC deberá acreditarse con presentación de la copia simple del certificado ISO27001 vigente.

5. Descripción de los servicios

5.1. SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA

5.1.1. 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.

El proveedor deberá brindar el presente servicio conforme lo siguiente:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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.
- 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 todo 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.
- 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 al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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.
- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

5.1.2. 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.

Detalles del Servicio:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos a este servicio.
- 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/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.
- 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 todo 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.
- 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 al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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 todas aquellas 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 integrados 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.
- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice A.

5.1.3. Servicios de Protección contra 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.

Detalles del Servicio:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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.
- 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 todo 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.
- 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 al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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), los 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 otros que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

5.1.4. Servicios de Redes Privadas Virtuales (VPN)

Descripción del servicio:
El Instituto requiere la continuidad operativa del servicio de interconexión a través de Internet que permitan establecer comunicación desde localidades remotas para la transferencia de información a través de un canal cifrado.

Detalles del Servicio:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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.

- 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 todo el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarios durante la vigencia de los servicios.
- 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 al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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.
- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

5.1.5. 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.

Detalles del Servicio:

ANEXOS
DIVISIÓN DE CONTRATOS

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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.
- 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 todo 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.
- 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 al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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.
- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

5.1.6. 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.

Detalles del Servicio:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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.
- Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes.
- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.

ANEXOS
DIVISIÓN DE CONTRATOS

- 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 todo 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.
- 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 al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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.
- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

5.1.7. 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.

Detalles del Servicio:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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.
- 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 todo 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.
- 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 al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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.
- Cumplir con las especificaciones técnicas y operativas descrito en el Apéndice A.

5.1.8. 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.

Detalles del Servicio:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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.
- 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 todo 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.
- 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 al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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.
- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

5.1.9. 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.

Detalles del Servicio:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.

ANEXOS

- 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 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.
- 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 los 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 todo 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.
- 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 al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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.

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

5.2. SERVICIOS DE SEGURIDAD – VERIFICACIÓN Y CALIDAD

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

5.2.1. Servicios de Análisis de Vulnerabilidades

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.

Detalles del Servicio:

- Integrar todas 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 solicitado.
- 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 permitan 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.

5.2.2. Servicios de Pruebas de Penetración

Descripción del servicio:

El Instituto requiere la continuidad de un servicio que permite 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.

Detalles del Servicio:

- 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 solicitado.
- Dar seguimiento a los servicios o activos de información que deberán ser analizados, incluyendo el número de equipos involucrados, y la versión de las plataformas de los sistemas analizados.
- Identificación de vulnerabilidades y malas configuraciones.
- Explotación de acceso a los sistemas mediante el aprovechamiento de los huecos de seguridad detectados y/o vulnerabilidades detectadas.
- Evaluación de vulnerabilidades de al menos los siguientes rubros:
    - Autenticación y Autorización
        - Intentos ilimitados de inicio de sesión
        - Insuficiente autenticación
        - Insuficiente autorización
    - Gestión de sesión
        - Predicción de sesión
        - Secuestro de sesión
        - Reproducir sesión
        - Expiración de sesión insuficiente
    - Inyección de código
        - Inyección comando de Sistema Operativo
        - Inyección SQL
        - Cross-site Scripting
        - Inyección LDAP
        - Inyección HTML
        - Parameters Tampering
        - Cookie Poisoning
        - Hidden Field Manipulation
    - Criptografía
        - Fortaleza del algoritmo
        - Gestión de llaves
    - Ataques Lógicos
        - Abuso de funcionalidades
        - Input Field Validation Checking
    - Protección de Datos
        - Transporte
        - Almacenamiento
    - Divulgación de Información
        - Indexado de directorio
        - Path Traversal

- Manejo inseguro de errores
- Comentarios HTML

- Realizar un reporte ejecutivo y técnico, por cada requerimiento atendido, en el que se describan los detalles de los riesgos asociados a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP llamada "OWASP Risk Rating Methodology", detallando recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.
- Integrar un proceso y/o procedimiento para la continuidad de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada.
- El proveedor de servicios deberá integrar el mecanismo operativo necesario para llevar a cabo el proceso de remediación conforme las vulnerabilidades reportadas, contemplando personal especializado para las plataformas operativas y herramientas en software descubiertas.

5.2.3. 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 identifican 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.

Detalles del Servicio:

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

5.2.4. Servicios de Borrado Seguro de Información

Descripción del servicio:

Se requiere dar continuidad a la solución de borrado seguro de información, para los dispositivos como son 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 de servicios, así como las entregas de información requeridas en el presente documento, deberán apegarse a la normativa vigente aplicable para dichos servicios y soluciones.

Detalles del Servicio:

- Integrar todas aquellas renovaciones que sean necesarias durante la vigencia de los servicios.
- Garantizar que las herramientas de borrado seguro cuenten con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios del servicio correspondiente.
- Deberá permitir realizar borrados completos en medios de almacenamiento dispuestos en activos de infraestructura como: equipos de cómputo (de escritorio y portátil), equipos de propósito específico (appliance), servidores físicos o virtuales, derivado de la sustitución, migraciones o retiro por finalización del contrato.
- Deberá asegurar que los datos no puedan ser recuperados, basándose en al menos los siguientes estándares internacionales
    - HMG Infosec Standard 5 (baseline and enhanced)
    - Opnavinst 5239.1A
    - Extended NIST 800-88
    - DoD 5220.22-M
    - ISO-IEC 15408
    - ECE y BSI/VSITR
- Borrado de Discos duros IDE/ATA, SCSI, SAS, USB, SATA, SSD, Fiber Channel y FireWire, de estado sólido y mecánicos de cualquier tamaño.
- Deberá brindar la destrucción local y/o remota en múltiples dispositivos de almacenamiento.
- Deberá posibilitar el desmontaje RAID (SCSI).
- Deberá permitir el borrado y detección de zonas bloqueadas / ocultas (DCO, HPA).
- Deberá generar certificados de borrado infalsificables que ofrezcan protección ante cualquier instancia legal, en donde se incluya el resultado del proceso de borrado, fecha, hora, los datos del equipo, el detalle del dispositivo de almacenamiento borrado.
- Deberá emitir una firma electrónica para la autenticación de la integridad del reporte de sanitización emitido por el *software* de borrado.
- La solución deberá ejecutarse sin importar de que sistema operativo se trate.
- El reporte que generé la solución deberá ser exportado a un medio de almacenamiento como USB o disco duro.

- El servicio de borrado seguro esta provisto mediante un proceso o flujo operativo, el cual deberá contemplar entre otros, los siguientes puntos:
  - Solicitud de borrado.
  - Identificación del medio de borrado.
  - Definición de fecha de borrado.
  - Flujos operativos para la autorización de borrado o destrucción.
  - Como referencia, se muestran los insumos a ser atendidos

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).

5.2.5. Servicio de Gestión de Dominios

Descripción del servicio:

Contar con la continuidad del servicio que permita registrar ante las instancias certificadas por el NIC, los dominios que requiera el Instituto y su correcta gestión.

Detalles del Servicio:

- 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 pagos que correspondan derivados del registro, cambio de dominio o proveedor sin costo adicional para el Instituto.

5.2.6. 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.

Detalles del Servicio

El servicio de certificados digitales SSL deberá comprender lo siguiente:

- Validación de dominios
- Encripción SSL de al menos 256 bits
- No debe de ser auto firmado, sino emitido por instancia certificadora valida (tercero confiable)
- El tiempo de emisión debe de ser menor a 24 Horas y hacerlo llegar al personal del Instituto.
- 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)

5.2.7. 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 27001, 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.

Detalles del Servicio:

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

Planear

- Capacitación de seguimiento – Curso "Inducción a la norma 27001:2013 o vigente.
  Curso que permita al participante:
    - 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 27001.
- Procesos de seguridad aplicables en la normativa vigente.
- Enfocarse a las áreas de TI y a los terceros que proveen servicios de TI al Instituto, considerando como alcance el catálogo de infraestructuras críticas del Instituto (al menos 20 directivas).

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

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

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

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

- Detalle y actualización de políticas y procedimientos de seguridad existentes

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

- Propuestas de implementación de los controles seleccionados.
  La metodología deberá considerar los siguientes temas:
  - Control de accesos

- Monitoreo de cuentas
- Definición del proceso de Continuidad del negocio
- Implantación de los Roles y responsabilidades definidas para el Sistema de Gestión de Seguridad de la Información
- Controles de seguridad en la infraestructura tecnológica de acuerdo con lo definido en el alcance.

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

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

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

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

- Acciones correctivas y no conformidades.
  Deberá considerar lo siguiente:
  - Apoyo en la definición y seguimiento del procedimiento para realizar acciones correctivas y no conformidades derivadas de las 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.

5.3. SERVICIOS DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

El Instituto requiere que el proveedor del servicio cuente con un Centro de Operaciones de la Seguridad (SOC), que se encuentre físicamente en las instalaciones del proveedor. El objetivo de este centro deberá de ser la continuidad operativa a la gestión de la seguridad, así como responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad, que ejecute actividades de revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, análisis forense, notificación de alertas y vulnerabilidades, así como el establecimiento de acciones de mejora sustentable.

El proveedor, 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 debe 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.

Detalles del Servicio:

- Ubicarse dentro de territorio nacional.
- 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 1 mes antes del término de estos.
- Realizar acciones correctivas y preventivas para asegurar la confidencialidad, integridad y disponibilidad de la información que se maneja en las diferentes soluciones se seguridad.
- Notificaciones y alertas personalizadas, en caso de desviaciones, anormalidades o brechas de seguridad, para cada una de las soluciones de seguridad.

- Revisiones continuas a la operación del SOC, que permitan establecer mejora en los procesos, procedimientos y controles de seguridad.
- Analizar los eventos de seguridad y administración de bitácoras que se integran en los servicios de correlación de información, a fin de establecer acciones preventivas a través de modificaciones a las configuraciones de las soluciones de seguridad.
- Integrar un Equipo de Atención y Respuesta a Incidentes de Seguridad.
- Soporte y Atención a fallas a los componentes hardware y software que integran la solución, conforme lo estipulado en los acuerdos de niveles de servicio.
- Monitorear la disponibilidad de los componentes hardware y software que integran la solución ofertada. La solución de monitoreo debe tener la capacidad de generar alertas y notificaciones en caso de fallas, degradación del desempeño de procesamiento de información, intermitencia y/o pérdida de disponibilidad.
- Realizar mantenimiento preventivo y correctivo a las soluciones de seguridad habilitadas, así como a los activos de infraestructura que soportan cada servicio.
- Ejecutar procesos operativos para al menos los siguientes rubros:
    - Administración de Dispositivos.
    - Administración de Requerimientos.
    - Administración de Cambios.
    - Administración de Configuraciones.
    - Administración de Vulnerabilidades.
    - Administración de Incidentes.
    - Administración de Problemas.
- Integración de una Mesa de servicio apegada a ITIL v4, la cual debe integrarse con la Mesa de Servicios Tecnológicos del Instituto, considerando todas las actividades de puesta a punto, desarrollo de piezas de software, configuraciones, entre otros, que permitan establecer la comunicación para la generación de requerimientos, cambios, incidentes, y otros procesos que determine el Instituto.
- El servicio de requerimientos, cambios, incidentes, entre otros, deberá permitir la generación de eventos (tickets), mediante los mecanismos que se establezcan en las mesas de trabajo correspondiente, que, de manera enunciativa más no limitativa, podrán ser:
    - Un número telefónico directo en las instalaciones del SOC.
    - Un número telefónico a diez dígitos.
    - Correo Electrónico
    - Portal Web
- El personal del proveedor del servicio, que atenderá las operaciones de los servicios de seguridad, deberá contar con experiencia probada en las áreas de tecnología y de seguridad de la información previamente mencionadas, para lo cual, deberá integrarse el currículo vitae de todo el personal que participe en el servicio, indicando al menos:
    - Experiencia profesional: bajo este rubro, se considerarán todos los puestos que cada integrante haya desempeñado, con fecha, nombre de los empleadores, nombre de los puestos que ha ejercido y el tipo de funciones bajo su responsabilidad, y deberá contar con experiencia comprobable al menos 5 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 5 años.
    - Estudios: bajo este rubro se anotarán todos los estudios en materia de seguridad de la información, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica. Las certificaciones son de tecnología y/o de seguridad de tipo "vendor-neutral".
    - Incluir la estructura del grupo de trabajo, indicando por cada perfil las responsabilidades y competencias.

- El Instituto podrá solicitar la revisión de la infraestructura de seguridad por un tercero en cualquier momento, durante la vigencia del contrato, con la finalidad de dar certeza de la entrega del servicio.
- Seguimiento a la Base de Datos de la Gestión de la Configuración (CMDB por sus siglas en ingles) que contenga los detalles relevantes de cada elemento de configuración (CI) y de la relación entre ellos, incluyendo el equipo físico, software y la relación entre incidencias, problemas, cambios y otros datos del servicio de seguridad.
- Generar los reportes de Inteligencia de Negocio y Analítica de Información que permitan tener estadísticas del uso y desempeño de los servicios de seguridad, esto último con el objetivo de coadyuvar a la toma de decisión estratégica y operativa de los servicios, así como para determinar el plan de capacidad de cada tecnología implementada. Dichos reportes podrán considerar, de manera enunciativa más no limitativa, la siguiente información:
  - Estadísticas de uso de procesamiento por tecnología
  - Estadísticas de desempeño por tecnología (throughput)
  - Estadísticas de ataques informáticos bloqueados.
  - Estadísticas de comportamientos tipo esperado de uso por tecnología (líneas base)
  - Estadísticas de usuarios concurrentes por servicio.
  - Estadísticas de crecimiento diario, mensual y anual por cada servicio.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración de los servicios de seguridad, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Las consolas de administración provistas para los servicios de seguridad deberán permitir visualizar al menos:
  - Políticas: Control de Acceso
  - Configuraciones: Listas de Control de Acceso (Listas Blancas, Listas negras), Líneas base de seguridad.
  - Objetos: Usuarios, Grupos, Direcciones IP
  - Bitácoras.
  - Estadísticas en tiempo real: Desempeño, procesamiento, usuarios conectados, conexiones por segundo, ancho de banda utilizado.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para cada solución o servicio, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso de los servicios de seguridad.
- Integrar un Tablero de Estadísticas de Servicios de Seguridad a través de un portal único de administración de los servicios de seguridad de forma independiente a las consolas de administración de los servicios de seguridad, así como de las herramientas de monitoreo que contenga información estratégicas sobre el uso de los servicios en tiempo real y de manera histórica, y que permita al Instituto tener el contexto general sobre el desempeño de las soluciones, su estado de salud, incidentes registrados, reportes de actividades sospechosas relevantes a nivel mundial, u otra información relevante que permita tomar decisiones sobre las condiciones de operación de los servicios, el licitante ganador debe incluir en su oferta económica los costos asociados al desarrollo para el cumplimiento de éste requerimiento.
- Permitir al personal que designe el administrador del contrato, generar reportes explotando todas las variables y funcionalidades de la herramienta de monitoreo, con la opción de parametrizar dichos reportes y consultarlos vía web.

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

PERFIL	CERTIFICACIONES A DEMOSTRAR	EXPERIENCIA A DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Administrador del Centro de Operaciones de Seguridad (SOC)	CISM (Certified Information Security Manager) o CISSP (Certified Information Systems Security Professional)	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 recurso
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.	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 recursos
Analista de Seguridad	CEH (Certified Ethical Hacker)	3 años de experiencia en participación de proyectos de seguridad de la información.	Encargado de ejecutar las revisiones de seguridad sobre las aplicaciones y la infraestructura, así como prever, detectar, analizar, contener, erradicar, documentar incidente de seguridad.	Al menos 2
Líder de proyecto	PMP (Project Manager Professional) Certificado por PMI o ITIL v4 (Expert o Master)	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	ITIL v4 Foundation Certification	3 años de experiencia en participación de proyectos de seguridad de la información.	Personal encargado de las operaciones de soporte de primer nivel, el monitoreo de los servicios, así como del registro y seguimiento de solicitudes de ventanas de mantenimiento, reportes de fallas y requerimientos.	Al menos 4

PERFIL	CERTIFICACIONES A DEMOSTRAR	EXPERIENCIA A DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Consultor de Penetración	GPEN (GIAC Certified Penetration Tester) o CEH (Certified Ethical Hacker) o CICP (Core Impact Certified Profesional)	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 recurso
Consultor Forense de Cómputo	EnCE (EnCase Certified Examiner) o 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 recurso

PERFIL	CERTIFICACIONES A DEMOSTRAR	EXPERIENCIA A DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Arquitecto Especializado en Redes y Seguridad	CCNP (Cisco Certified Network Professional) o CCSP	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 fallos e incidentes que se presenten en la interoperabilidad con otros proveedores y/o fabricantes.	Al menos 1 recurso

6. 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.

6.1. 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.

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto	Única Vez	15 días naturales posterior a la notificación de adjudicación
	Documento Compromiso de suscripción del acuerdo de niveles operacional (*Operational Level Agreement*, OLA	Única Vez	15 días naturales posterior a la notificación de adjudicación

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Matriz de Escalación	Única Vez	15 días naturales posterior a la notificación de adjudicación
	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 posterior a la notificación de adjudicación
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	Único Vez	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las 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	Única Vez	5 días hábiles posteriores a la integración de las

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integran activos de infraestructura para su habilitación		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 intraestructura para su habilitación	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad, que requieran integran activos de infraestructura para su habilitación	Única Vez	20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados
Servicios de Análisis de Vulnerabilidades	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Pruebas de Penetración	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Análisis Forense	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Borrado Seguro de Información	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
			integración de las mesas de trabajo
Servicio de Gestión de Dominios	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicio de Certificados Digitales SSL	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior 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 posterior a la integración de las mesas de trabajo
Servicios del Centro de Operaciones de Seguridad (SOC)	Procesos de operación implementados: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	Única Vez	15 días naturales posterior a la a la notificación de adjudicación
	Matriz de Escalación Técnica y Organizacional	Única Vez	15 días naturales posterior a la a la notificación de adjudicación
	Procedimiento de operación de la Mesa de Servicios: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	Única Vez	15 días naturales posterior a la a la notificación de adjudicación
	Plan de Recuperación en caso de desastre (DRP)	Única Vez	60 días naturales posterior a la integración de las mesas de trabajo
	Expedientes Curriculares del personal del SOC	Única Vez	15 días naturales posterior 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

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
			cada solución integrada y posterior a la integración de las mesas de trabajo

6.2. Entregables bajo demanda

El proveedor, de manera enunciativo más no limitativo, deberá generar entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades	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 posterior 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	Evento	10 días hábiles posterior a la solicitud generada por parte del Instituto

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis		
Servicios de 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 posterior a la solicitud generada por parte del Instituto
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:	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado.		
Servicio de Gestión de Dominios	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos.	Evento	5 días hábiles posterior 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 posterior a la solicitud generada por parte del Instituto
Servicios de Sistema de Gestión de Seguridad de la Información	Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo	Evento	10 días hábiles posterior 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 nábiles posterior 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 posterior 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 posterior a la incorporación o sustitución de nuevo

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
			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 posterior 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 posterior 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 posterior a la solicitud generada por parte del Instituto
	Reporte Técnico de los requerimientos registrados en la mesa de servicios	Evento	5 días hábiles posterior 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 posterior a la solicitud generada por parte del Instituto
	Diagramas de Arquitectura de las soluciones de seguridad y red	Evento	2 días hábiles posterior a la solicitud generada por parte del Instituto

6.3. 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:

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Seguridad – Continuidad Operativa	Reportes Técnicos de los activos de infraestructura que contemplen: • 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 posterior al cumplimiento del mes vencido
Servicios de Seguridad – Verificación/Calidad	Reportes Técnicos de los activos de infraestructura que contemplen: • 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 posterior al cumplimiento del mes vencido
Servicios de Red – Continuidad Operativa	Reportes Técnicos de los activos de infraestructura que contemplen: • 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 posterior 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 posterior al cumplimiento del mes vencido
	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posterior 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 posterior al cumplimiento del mes vencido
	Reporte de las evaluaciones operativas a los servicios de seguridad implementados	Trimestral	5 días hábiles posterior 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 posterior al cumplimiento de cada trimestre calendario

Los entregables requeridos durante la vigencia del contrato, deberán ser entregados en formato electrónico (MS Word, MS Excel, PDF) conforme los periodos estipulados por el Instituto.

De igual manera, el proveedor deberá establecer un repositorio digital, que, de manera alterna, servirá para alojar los entregables antes señalados, mismos que estarán disponibles para su consulta durante la vigencia del contrato, teniendo en cuenta que el Instituto definirá en las mesas de trabajo los permisos de acceso correspondientes para el administrador del contrato, cuerpo de gobierno que se conforme para este propósito u otros funcionaros que sean designados por el primero mencionado.

7. NIVELES DE SERVICIOS

Los Niveles de Servicio, así como penas convencionales y deducciones, se aplicarán conforme a lo estipulado en el documento denominado "Términos y Condiciones".

8. CONVENIO DE CONFIDENCIALIDAD Y RESGUARDO DE LA INFORMACIÓN

El Proveedor de los servicios de seguridad deberá actualizar y firmar el Convenio de Confidencialidad y Resguardo de Información correspondiente. Así mismo, deberá considerar al menos los siguientes mecanismos de control de acceso a la información del Instituto:

- Se deberán establecer controles de acceso y privilegios restringidos al personal del Proveedor, con el fin de reservar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del Instituto.
- Se deberá implantar y aceptar en todo momento el uso de controles que permitan registrar "Pistas de Auditoria" para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.
- La seguridad lógica deberá estar protegida mediante el uso de dispositivos de control de acceso (Firewalls), mecanismos de encriptación y seguridad física entre las redes del Proveedor del SASI-C y las del Instituto.
- Los empleados del Proveedor, con acceso a la información sensible del Instituto, deberán firmar acuerdos de confidencialidad con este último.
- El almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por el proveedor de los servicios, observando los requisitos de seguridad y resguardo de la información.
- El Proveedor de servicios, permitirá el acceso a información relacionada con el servicio prestado al Instituto para la realización de auditorías.
- El Proveedor de servicios 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.

9. 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 realice 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:

- El 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.
- Normas ISO/IEC27001:2013 o vigente (Copia simple a nombre de proveedor participante)

9.1. Cumplimiento de Políticas

El Proveedor de servicios deberá respetar todas las políticas de seguridad vigentes en el Instituto y en ninguna circunstancia deberá permitir que se viole ninguno de los lineamientos vigentes. Si alguno de los lineamientos de Seguridad implantados en el Instituto llegase a cambiar en el transcurso del contrato establecido con el Proveedor, éste deberá asegurarse de modificar su infraestructura y procesos de tal forma que cumpla con los nuevos requerimientos.

Todos los equipos de cómputo personal propiedad del proveedor de servicios, que estén involucrados en la prestación de los servicios, deberán estar protegidos con sistemas de detección de intrusos, control de infecciones virales, detección y eliminación de programas tipo "back door" o "Troyanos". Esta regla aplica tanto para los equipos de cómputo móviles (laptops, handheld, smartphones, tablet PC, etc.) como para los equipos de escritorio (desktop, deskside, etc.) usados por los recursos designados para las diversas tareas de administración y gestión.

Si dichos equipos requirieran de la instalación de sistemas operativos, aplicaciones, sistemas antivirus, sistemas de seguridad y demás herramientas que el proveedor decida 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.

9.2. Consideraciones en la finalización del Contrato

La infraestructura, los componentes habilitadores y los demás elementos utilizados por el proveedor para la prestación de los servicios se transferirán al IMSS para la continuidad operativa. Este acto se llevará a cabo mediante un acta de entrega recepción, en la que dichos componentes se transmitirán al IMSS, a título gratuito, libres de toda limitación de dominio, gravamen y responsabilidad de cualquier naturaleza, conforme a la normativa aplicable al Instituto.

El Proveedor deberá entregar al Instituto, a más tardar 2 meses antes de la finalización del Contrato, un plan de trabajo detallado para lograr una transición efectiva, en el que se incluyan todos los hitos y plazos necesarios 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.
En el caso de celebrarse un convenio modificatorio que amplíe el tiempo originalmente pactado, el proveedor deberá acordar mediante mesa de trabajo con el administrador del contrato, el plazo en que habrá de llevarse a cabo esta actividad.

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 Instituto solicite se mantengan para la transición de un nuevo contrato de servicios, procurando afectar de forma mínima la operación.

El Proveedor deberá garantizar los Niveles de Servicio durante transición a un nuevo proveedor. Asimismo, al término del contrato, garantizará los Niveles de Servicio durante el periodo de transferencia de servicios al nuevo proveedor.

ANEXOS

Dicho periodo de transición estará sujeto al Plan de Trabajo que el Proveedor haya presentado previamente, y que el Instituto hubiera aprobado. No obstante, durante dicho periodo, el Proveedor deberá proporcionar la orientación tecnológica adecuada al personal del Instituto para garantizar la continuidad de los servicios requeridos, poniendo a disposición de un tercero la transferencia o quien el Instituto designe para dicho propósito.

9.3. Condiciones posteriores al término del Contrato

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.

10. 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.

11. CLAVE CUCoP

31904

12. REQUERIMIENTOS DE ARQUITECTURA TECNOLÓGICA

No Aplica

13. RESTRICCIONES E INTERFACES CON OTROS ELEMENTOS

No Aplica

14. UNIDAD DE MEDIDA

Servicios

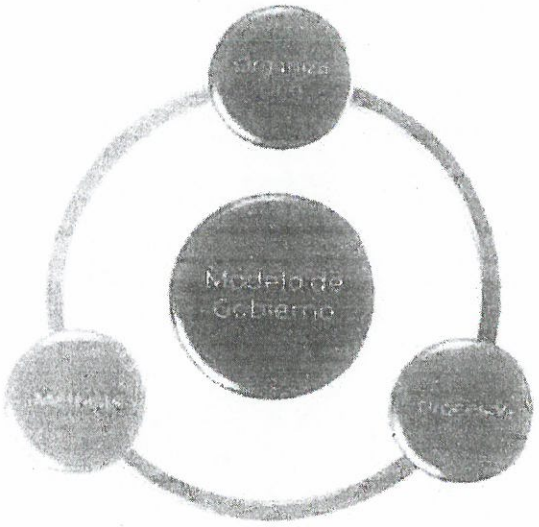
15. MODELO DE GOBIERNO SASI-C

El Modelo de Gobierno establece la forma como se trabajará en relacion 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 Continuidad (SASI-C)", 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 a fin de en cada una de las etapas del servicio, el del Administrador del Contrato y los Lideres del proyecto, con apoyo por parte del proveedor del servicio (SOC), aseguren los niveles de servicios establecidos para la operación.

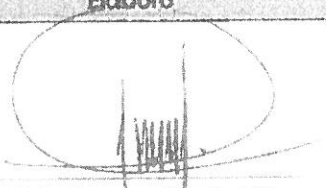


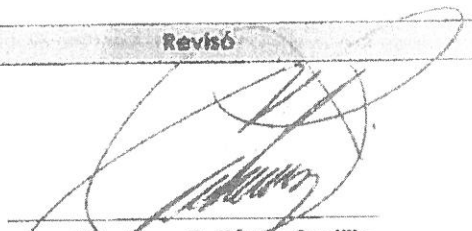
La estructura organizacional que ejecutar para el proyecto de "Servicios Administrados de Seguridad Informática Continuidad (SASI-C)", busca que los responsables trabajen de manera efectiva, definiendo roles y responsabilidades en cada nivel, para lo cual se muestra en la siguiente tabla de manera enunciativa mas no limitativa a los responsables y sus roles correspondientes.

NIVELES ORGANIZACIONALES	RESPONSABLES	DESCRIPCIÓN
Supervision 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.
Lider 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"

ANEXOS
DIVISIÓN DE CONTRATOS

16. FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaboró

Lic. Cynthia Osmara Verdin Villegas
Jefe Área Nivel Central.

Revisó

Ing. Abraham Gutiérrez Castillo
Titular de la División de Seguridad Informática Física.

Aprobó

Lic. Florencio Fernando González Velázquez
Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información.

INSTITUTO MEXICANO DEL SEGURO SOCIAL

DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

COORDINACIÓN DE TELECOMUNICACIONES Y SEGURIDAD DE LA INFORMACIÓN

TERMINOS Y CONDICIONES

SERVICIOS ADMINISTRADOS

DE SEGURIDAD INFORMÁTICA CONTINUIDAD (SASI-C)

Índice

ANEXOS
DIVISIÓN DE CONTRATOS

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
0.1	Septiembre 30 2021	Actualización del Documento	Lic. Cynthia Osmara Verdin Villegas
0.2	Septiembre 30 2021	Revisión del Documento	Ing. Abraham Gutierrez Castillo
1.0	Septiembre 30 2021	Autorización del Documento	Lic. Florencio Fernando González Velázquez

1. OBJETIVO DEL DOCUMENTO

Establecer las necesidades y condiciones de entrega los Servicios Administrados de Seguridad Informática Continuidad (SASI-C).

2. PREMISA

Las bases de datos, aplicaciones y cualquier otro tipo de información utilizado en el suministro de los servicios o a la que se tenga acceso derivado de la naturaleza de los mismos, 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 a "EL INSTITUTO".

3. NOMBRE DEL PROYECTO

Servicios Administrados de Seguridad Informática Continuidad (SASI-C)

4. OBJETIVO 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 garanticen la continuidad operativa, de negocios y de seguridad de la información del Instituto que:

1. Garantice la continuidad operativa, la continuidad del negocio y la continuidad de la seguridad de la información de la Institución, durante la vigencia del presente contrato, especialmente durante la toma de operación y la transición de los servicios de los contratos anteriores (SASI) a los servicios propios de SASI-C.

2. 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, y contención de ataques que puedan presentarse en la infraestructura de cómputo, sistemas y aplicaciones del Instituto.

3. Cuente con servicios de infraestructura regulados por niveles de servicio, que: implementen (instalen, migren habiliten y pongan a punto) los componentes

necesario en los Centros de Datos del Instituto 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.

4. 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, protección, pruebas, metodologías, de distintos rubros como el de acceso a cuentas privilegiadas, base de datos, aplicaciones, fuentes múltiples, vulnerabilidades, investigación forense y de procesos de seguridad, así como con otros servicios especializados en materia de seguridad y tecnologías de la información.

5. Cuente con servicios de soporte extendido que son necesarios para posibilitar y articular los Servicios Administrados de Seguridad Informática Continuidad (SASI-C).

Contar con los **Servicios Administrados de Seguridad Informática Continuidad** para los activos de Información donde se alojan los aplicativos, sistemas de información y bases de datos sensibles del instituto, en las ubicaciones en donde los requiera el instituto, así como con los niveles de servicio establecidos en el apéndice del presente documento y conforme a las características técnicas solicitadas en el Anexo Técnico.

5. SOLICITUD DE APEGO A NORMAS OFICIALES O CERTIFICACIONES

Se Indica específicamente en el punto 9 del Anexo Técnico del presente proyecto.

6. VISITAS A INSTALACIONES

No se requiere.

7. TIPO DE ABASTECIMIENTO REQUERIDO

El tipo de abastecimiento será mediante partida única.

8. GARANTÍAS

El Proveedor, se obliga a constituir en la forma y términos previstos por los artículos 48 y 49 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 103 de su Reglamento y numerales 4.30 y 4.30.3 de las Políticas, Bases y Lineamientos en materia de

Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social, la garantía de cumplimiento divisible correspondiente.

En cualquier momento, "EL INSTITUTO" podrá hacer válida la Póliza de Garantía del contrato en caso de que el proveedor no cumpla con los tiempos y plazos de entrega establecidos en los presentes Términos y Condiciones.

Las modificaciones a las fianzas deberán formalizarse con la participación que corresponda a la afianzadora, en términos de las disposiciones aplicables.

La garantía permanecerá vigente a partir de la fecha de adjudicación del contrato respectivo, y hasta que se cumplan plenamente todas y cada una de las obligaciones del contrato, así como durante la substanciación de todos los recursos legales o juicios que, en su caso, sean interpuestos por cualquiera de las partes y hasta que se dicte la resolución definitiva por autoridad competente.

Para garantizar el cumplimiento de todas y cada una de las obligaciones estipuladas en el contrato Adjudicado, el proveedor se compromete a entregar, dentro de los 10 (diez) días naturales a partir del día siguiente al de la notificación de la adjudicación del inicio de los servicios la garantía en los términos aquí señalados, 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.

ANEXOS
DIVISIÓN DE CONTRATOS

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.

9. ACUERDOS DE NIVEL 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 de sean proporcionados con la calidad prevista.

Con fundamento en lo dispuesto por el Artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el Instituto aplicará penas convencionales por el atraso en la prestación del servicio basado en el importe del servicio prestado con atraso conforme al plan de trabajo y los plazos previstos, en el entendido de que esta penalización no excederá al importe de la garantía de cumplimiento de contrato.

9.1. 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 en la prestación del servicio, respecto del valor máximo total del contrato.

9.2. Servicios de Habilitación, Operación y Transición

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	CÓMPUTO DE LA PENALIZACIÓN
Plan de Trabajo detallado de los servicios del proyecto	15 días naturales posteriores a la notificación de adjudicación	1% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Documento Compromiso de suscripción de OLA	15 días naturales posteriores a la notificación de adjudicación	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 notificación de adjudicación	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 deciare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	15 días naturales posteriores a la notificación de adjudicación	1% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

ANEXOS
DIVISIÓN DE CONTRATOS

9.3. Servicios de Seguridad – Continuidad Operativa

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	CÓMPUTO DE LA PENALIZACIÓN
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 las Servicios de Seguridad	20 días hábiles previo al termino 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

9.4. Servicios de Seguridad – Verificación/Calidad

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	COMPUTO DE LA PENALIZACIÓN
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
Memorias Técnicas Actualizadas de las Servicios de Seguridad que	20 días hábiles previo al termino del contrato para aquellos servicios	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado

ANEXOS
DIVISIÓN DE CONTRATOS

requieran integran activos de infraestructura para su habilitación	que se encuentren habilitados		con el incumplimiento
Procedimientos de Operación del servicio • Servicio de Análisis de Vulnerabilidades dinámico • Servicios de Pruebas de Penetración • Servicios de Análisis Forense • Servicios de Borrado Seguro de Información • Servicio de Gestión de Dominios • Servicio de Certificados Digitales SSL	10 días hábiles 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
Metodología para la continuidad de los servicios • Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)	10 días hábiles 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

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

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	CÓMPUTO DE LA PENALIZACIÓN
Procesos de operación	15 días naturales posterior a la	2% por cada día natural de atraso	Valor unitario de la facturación

Implementados: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	notificación de adjudicación		mensual del servicio relacionado con el incumplimiento
Matriz de Escalación Técnica y Organizacional	15 días naturales posteriores a la notificación de adjudicación	2% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Procedimiento de operación de la Mesa de Servicios: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	15 días naturales posteriores a la notificación de adjudicación	2% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Plan de Recuperación en caso de desastre (DRP)	60 días naturales posterior a la integración de las mesas de trabajo	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 posteriores a la notificación de adjudicación	2% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

9.6. Deducciones

Durante la vida 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-C,

siempre y cuando demuestre con evidencias fehacientes que el servicio correspondiente se presentó bajo las especificaciones del anexo técnico y sus apéndices.

Con base en lo anterior, y cuando las fallas, incidentes, atención de requerimientos, ventanas de mantenimiento, entre otras, sean atribuibles a la entrega de los servicios de seguridad por parte del Proveedor, se aplicarán deductivas conforme lo siguiente rubros:

9.7. Disponibilidad

La disponibilidad se define como la medida del porcentaje de tiempo, en que el sistema que brinda el servicio de seguridad de SASI-C (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-C 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-C, para todos los módulos o posiciones de servicio contratados.

El Proveedor de SASI-C 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-C, restándosele aquellos períodos de indisponibilidad cuya responsabilidad no sea atribuible al Proveedor de SASI-C. 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-C.
    - Disponibilidad por sitio y por Posición de Servicio

Las caídas originadas por falla de energía responsabilidad del Instituto no serán tomadas en cuenta para la disponibilidad.

$$\text{Disponibilidad\_del\_Servicio} = \left\{ \frac{\text{Tiempo\_Total} - (\text{Tiempo\_Indisponible} - \text{Tiempo\_Instituto})}{\text{Tiempo\_Total}} \right\} \times 100$$

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:

Disponibilidad Servicio	% Disponibilidad
Servicios de Seguridad – Continuidad Operativa	99.99%
Servicios de Seguridad – Verificación y Calidad	99.97%
Servicios del Centro de Operaciones de Seguridad (SOC)	99.99%

Deductiva por incumplimiento:

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
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

9.8. Tiempo de Detección y Solución de Fallas

ANEXOS
DIVISIÓN DE CONTRATOS

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-C usando su correspondiente herramienta de gestión y monitoreo del servicio. El Proveedor deberá realizar esta medición en un periodo mensual considerando el promedio del tiempo de solución para cada tipo de severidad. La metodología que se realice, las herramientas y los responsables sobre las mediciones, quedarán definidos en las mesas de trabajo.

El Tiempo de Solución a Fallas se divide en tres casos, en función de la severidad, causa e impacto de los mismos:

Severidad Critica: Representa un incidente de alto impacto dado el riesgo que representa. Este tipo de incidente puede, potencialmente, ocasionar afectación y daño en activos y servicios del cliente. Eventos de afectación total al servicio, pérdida total del sistema de comunicaciones y/o seguridad, degradación de los recursos del Instituto o bien mediante el descubrimiento de vulnerabilidad en la infraestructura protegida. La alarma relativa en el sistema de gestión se mantiene por más de 10 minutos.

Severidad Alta: Representa un incidente serio en el que hay una degradación más no una afectación de negocio a los servicios e infraestructura que es protegida mediante los dispositivos de alta disponibilidad o de seguridad. El incidente se manifiesta mediante el bloqueo o bajo desempeño al acceder a ciertos servicios de red que requieren el uso de los dispositivos de comunicaciones y/o seguridad, así como la pérdida parcial de alguna funcionalidad en el equipo de comunicaciones y/o seguridad. Eventos de afectación que ocasionan degradación en el servicio sin llegar a ocasionar caída del mismo.

Severidad Media: Representa un incidente menor que no trae consecuencias de impacto de negocio a los servicios e infraestructura protegida por los dispositivos de seguridad. El incidente se da mediante fallas en visualización de bitácoras o problemas para comunicación de servicios internos del Instituto y hacia un grupo reducido de usuarios. Eventos de afectación al servicio por períodos de tiempo menores a 10 minutos ocasionando intermitencia en la disponibilidad del servicio.

Severidad Baja: Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad. Estos casos de severidad deben ser atendidos por ingenieros del proveedor de servicios en sitio con la colaboración del fabricante vía un centro de asistencia técnica personalizada. El tiempo de resolución de este tipo de falla será definido por el Instituto y el Proveedor de SASI-C 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 posterior a la detección de la falla	2 horas posterior al registro y notificación de la falla
Alta	Representa una falla en la que hay una degradación que impide la operación de un servicio, mismo que soporta una función de negocio del Instituto pero que no tiene un impacto a nivel nacional.	20 minutos posterior a la detección de la falla	4 horas posterior al registro y notificación de la falla
Media	Representa una falla menor que impide la operación de un servicio, mismo que afecta a un grupo de usuarios reducido del Instituto.	120 minutos posterior a la detección de la falla	48 horas posterior al registro y notificación de la falla
Baja	Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad, tienen un bajo impacto en la operación del negocio y su atención y/o solución puede ser calendarizada.	5 días hábiles posterior a la detección de la falla	Se define entre el Instituto y el Proveedor de SASI-C conforme las mesas de trabajo que se establezcan para este propósito.

Deductiva por incumplimiento:

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO

ANEXOS
DIVISIÓN DE CONTRATOS

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LÍMITE DE INCUMPLIMIENTO
Tiempo máximo de registro y notificación conforme al nivel de severidad crítica	10 minutos posterior al registro y notificación de la falla	Minuto	0.1% 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 posterior al registro y notificación de la falla	Hora	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad alta	20 minutos posterior al registro y notificación de la falla	Minuto	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad alta	4 horas posterior 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 posterior al registro y notificación de la falla	Minuto	0.1% 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 posterior al registro y notificación de la falla	Hora	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel	5 días hábiles posterior al registro y notificación de	Día	0.1% por cada día hábil de atraso en el registro y	Valor unitario de la facturación mensual del servicio

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
de severidad baja	la falla		notificación	relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad baja	Se define entre el Instituto y el Proveedor de SASI-C conforme las mesas de trabajo que se establezcan para este propósito.	Día	0.5% por cada día de atraso en la solución de la falla conforme la fecha establecida en las mesas de trabajo	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

9.9. Tiempo de Detección y Mitigación de Incidentes

Una actividad sospechosa son acciones que pudieran estar encaminadas a comprometer la seguridad de la red y de los activos de información, es la etapa previa a la materialización de un incidente de seguridad. Un incidente de seguridad es el registro de una violación a las políticas de seguridad informática o al uso aceptable de políticas o de prácticas de seguridad estandarizado; es la evidencia inequívoca de que la confidencialidad, integridad y disponibilidad de la información ha sido vulnerada.

Las métricas de tiempo para la actividad sospechosa se refieren al tiempo de notificación y envió de dictamen que el proveedor SASI-C deberá realizar ante el Instituto al momento de detectar una actividad sospechosa. Ante una actividad sospechosa, el proveedor del SASI-C 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-C 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-C deberá detener y aislar el mismo según los tiempos definidos para cada prioridad.

Las mediciones deberán ser realizadas por el proveedor de SASI-C 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 un servicio, mismo que soporta una función de negocio del Instituto a nivel nacional.	10 minutos posterior a la detección del incidente	60 minutos posterior al registro y notificación del incidente
Alta	Representa un incidente en el que hay una degradación que impide la operación de un servicio, mismo que soporta una función de negocio del Instituto pero que no tiene un impacto a nivel nacional.	20 minutos posterior a la detección del incidente	240 minutos posterior 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 posterior al registro y notificación del incidente
Baja	Son casos considerados como preventivos para fines de mejora u	60 minutos posterior a la detección del	2,880 minutos posterior al registro y notificación del

SEVERIDAD	AFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
	optimización de cualquier servicio de seguridad, tienen un bajo impacto en la operación del negocio y su atención y/o solución puede ser calendarizada.	incidente	incidente

Deductiva por incumplimiento:

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Registro y notificación de Actividad Sospechosa	30 minutos posterior 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 posterior 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	LIMITE DE INCUMPLIMIENTO
Tiempo máximo de registro y notificación conforme al nivel de severidad crítica	10 minutos posterior 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

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Tiempo máximo de solución conforme al nivel de severidad crítica	60 minutos posterior 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 alta	20 minutos posterior 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 alta	240 minutos posterior 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 posterior 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 posterior 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 posterior 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 posterior al registro y notificación del	Minuto	1% por cada minuto de atraso en la solución del	Valor unitario de la facturación mensual del servicio

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
	incidente		incidente	relacionado con el incumplimiento

9.10. Solicitudes de Requerimientos y Cambios

Es el tiempo que tarda el Proveedor de SASI-C en realizar una alta, cambio o baja sobre la infraestructura del servicio en seguridad, basada en el menú de configuraciones comunes preestablecidas durante las mesas de trabajo correspondientes. Estas configuraciones deberán ser acorde a las necesidades de conectividad y flujos de información de las aplicaciones del Instituto, entendiendo que la complicación para su atención es menor dado que se tiene la experiencia y el conocimiento de las mismas configuraciones de los módulos de los servicios de seguridad en operación.

Objetivos de la métrica:

Requerimientos

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 posterior a la solicitud formal por parte del Instituto	60 minutos posterior al registro realizado por el Instituto
Media	Requerimiento generado por parte del Instituto a fin de atender a necesidades de operación comunes.	30 minutos posterior a la solicitud formal por parte del Instituto	480 minutos posterior al registro realizado por el Instituto
Baja	Requerimiento generado por parte del Instituto a fin de atender a necesidades de operación programadas.	60 minutos posterior a la solicitud formal por parte del Instituto	1,440 minutos posterior al registro realizado por el Instituto

Cambios

PRIORIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE EJECUCIÓN
Emergente	Cambios requeridos como resultado de una pérdida repentina del servicio, falla en un activo de infraestructura o a petición del Instituto.	1 hora posterior a la solicitud formal por parte del Instituto	Conforme al plan de trabajo definido entre el Instituto y el Proveedor
Normal	Cambios solicitados para mejorar o restaurar un servicio o ampliar un activo de infraestructura, que no están considerados en el catálogo de cambios estándar, mismos que deben ser analizados y aprobados por el Instituto.	1 hora posterior a la solicitud formal por parte del Instituto	Conforme al plan de trabajo definido entre el Instituto y el Proveedor
Estándar	Cambios en los servicio 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 posterior 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:

Requerimientos

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Tiempo máximo de registro y notificación conforme al nivel de prioridad Alta	10 minutos posterior al registro y notificación del requerimiento	Minuto	0.1% 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 posterior 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 posterior al registro y notificación del requerimiento	Minuto	0.1% 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 posterior 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 posterior al registro y notificación del requerimiento	Minuto	0.1% 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	24 horas posterior al registro y	Hora	0.5% por cada hora o fracción de atraso en la	Valor unitario de la facturación mensual del

ANEXOS
DIVISIÓN DE CONTRATOS

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
de prioridad Baja	notificación del requerimiento		ejecución del requerimiento	servicio relacionado con el incumplimiento

Cambios

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Tiempo máximo de registro y notificación conforme al nivel de prioridad Emergente	60 minutos posterior al registro y notificación del cambio	Minuto	0.1% 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	5% 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 posterior al registro y notificación del cambio	Minuto	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Normal	Conforme al plan de trabajo definido entre el Instituto y el Proveedor	Hora	5% 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	60 minutos posterior al registro y notificación del cambio	Minuto	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Estándar				incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Estándar	24 horas posterior al registro y notificación del cambio	Hora	5% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

9.11. Servicios de Seguridad – Continuidad Operativa

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Reportes Técnicos de los activos de infraestructura que contemplen: • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	5 días hábiles posterior 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

9.12.Servicios de Seguridad – Verificación/Calidad

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LÍMITE DE INCUMPLIMIENTO
Reportes Técnicos de los activos de infraestructura que contemplen: • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	5 días hábiles posterior 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
Servicios de Análisis de Vulnerabilidades: 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	7 días hábiles posterior a la solicitud generada por parte del Instituto	Día	2% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
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	10 días hábiles posterior a la solicitud generada por parte del Instituto	Día	2% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LÍMITE DE INCUMPLIMIENTO
de las herramientas tecnológicas utilizadas para el proceso de análisis				
Servicios de Análisis Forense: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de infraestructura verificados	15 días hábiles posterior a la solicitud generada por parte del Instituto	Día	2% 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 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	5 días hábiles posterior a la solicitud generada por parte del Instituto	Día	2% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LÍMITE DE INCUMPLIMIENTO
incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado.				
Servicio de Gestión de Dominios: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos.	5 días hábiles posterior a la solicitud generada por parte del Instituto	Día	2% 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 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	2% 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 Análisis de Vulnerabilidades: Reporte Técnico y	10 días hábiles posterior a la solicitud generada por	Día	2% por cada día hábil de atraso en la entrega de los reportes	Valor unitario de la facturación mensual del servicio

ANEXOS
DIVISIÓN DE CONTRATOS

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada aplicación o grupo de aplicaciones 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	parte del Instituto		técnicos/ejecutivos	relacionado con el incumplimiento
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 posterior a la solicitud generada por parte del Instituto	Día	2% 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	Conforme a la fecha	Día	2% por cada día hábil de atraso en	Valor unitario de la facturación

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Seguridad de la Información: Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora del Sistemas De Gestión de Seguridad de la Información (SGSI)	estipulada en el plan de trabajo acordado entre el Instituto y el Proveedor		la entrega de los reportes de actividades, por periodo, por evento	mensual del servicio relacionado con el incumplimiento

9.13.Servicios de Red – Continuidad Operativa

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Reportes Técnicos de los activos de infraestructura que contemplen: • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	5 días hábiles posterior 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

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

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	5 días hábiles posterior 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 posterior 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 posterior 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 posterior 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	5 días hábiles posterior al cumplimiento del mes vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LÍMITE DE INCUMPLIMIENTO
los servicios de seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo				
Reporte de las evaluaciones operativas a los servicios de seguridad implementados	5 días hábiles posterior 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 posterior 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 posterior 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 posterior al término de la implementación de cualquier solución de seguridad o conforme a cada	Día	1% por cada día hábil de atraso en la entrega de las cuentas de acceso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
	solicitud generada por el Instituto			
Actualización de la matriz de escalación	5 días hábiles posterior 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 posterior a la ejecución de la ventana mantenimiento	Día	2% 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 posterior a la solicitud generada por parte del Instituto	Día	2% 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 posterior a la solicitud generada por parte del Instituto	Día	2% 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 posterior a la solicitud generada por parte del Instituto	Día	2% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de los requerimientos	5 días hábiles posterior a la solicitud	Día	2% por cada día hábil de atraso en la entrega	Valor unitario de la facturación mensual del

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LÍMITE DE INCUMPLIMIENTO
registrados en la mesa de servicios	generada por parte del Instituto		del reporte técnico	servicio relacionado con el incumplimiento
Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y su diagrama de interrelación conforme fueron registrados en la CMDB	5 días hábiles posterior a la solicitud generada por parte del Instituto	Día	2% 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 posterior a la solicitud generada por parte del Instituto	Día	2% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tablero de Estadísticas de Servicios de Seguridad (Portal Único)	10 días hábiles posteriores al término de la habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo	Día	2% 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

ANEXOS
DIVISIÓN DE CONTRATOS

incidente de seguridad, mismo que será clasificado con base en las afectaciones o riesgos que pudieron generar.

10. CONDICIONES DE PAGO

El administrador de contrato será el servidor público responsable de administrar y supervisar el cumplimiento de las obligaciones pactadas en el mismo.

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, será el responsable de recibir y aceptar cada uno de "Los Servicios" , así como realizará los trámites de pago en cumplimiento al procedimiento administrativos vigente en "EL INSTITUTO".

Para proceder a la liberación de pago, el Titular 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 contractuales a cargo del proveedor, así como de la ejecución, validación, técnica y administrativa de todos y cada uno de los documentos que acreditan que los servicios proporcionados por el proveedor se cumplieron en tiempo, forma y cantidad y que cumplen con las características, especificaciones y condiciones requeridas, procederá el pago de conformidad con lo establecido en el artículo 51 de la LAASSP.

La forma de pago al proveedor será la estipulada en el contrato y quedará sujeta a las condiciones que establezcan las mismas; sin embargo, no podrá exceder de veinte días naturales contados a partir de la entrega de la factura respectiva, previa entrega de certificado de licencia o de la prestación de los servicios en los términos del contrato.

El proveedor deberá entregar en la División de Trámite de Erogaciones, situada en la calle de 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, a mes vencido conforme a las entregas programadas.

11. 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:

11.1. Entregables Generales

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 notificación de adjudicación
	Documento Compromiso de suscripción de OLAs	Única Vez	15 días naturales posteriores a la notificación de adjudicación
	Matriz de Escalación	Única Vez	15 días naturales posteriores a la notificación de adjudicación
	Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades,	Única Vez	15 días naturales posteriores a la notificación de adjudicación

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	competencias y capacidades para soportar la prestación de los servicios		
Servicios de Seguridad - Continuidad Operativa	Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad	Única Vez	20 días hábiles previo al termino del contrato para aquellos servicios que se encuentren habilitados
Servicios de	Documento con el	Única Vez	5 días hábiles

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Seguridad – Verificación/Calidad	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		posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integran activos de infraestructura para su habilitación	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad, que requieran integran activos de infraestructura para su habilitación	Única Vez	20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados
Servicios de Análisis	Procedimientos de	Única Vez	10 días hábiles

ANEXOS
DIVISIÓN DE CONTRATOS

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
de Vulnerabilidades	Operación del servicio		posterior a la integración de las mesas de trabajo
Servicios de Pruebas de Penetración	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Análisis Forense	Procedimientos de Operación del servicios	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Borrado Seguro de Información	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicio de Gestión de Dominios	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicio de Certificados Digitales SSL	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)	Metodología de implementación de los servicios	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios del Centro de Operaciones de Seguridad (SOC)	Procesos de operación implementados: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	Única Vez	15 días naturales posteriores a la notificación de adjudicación
	Matriz de Escalación Técnica y Organizacional	Única Vez	15 días naturales posteriores a la notificación de adjudicación
	Procedimiento de operación de la Mesa de Servicios:	Única Vez	15 días naturales posteriores a la

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	• Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo		notificación de adjudicación
	Plan de Recuperación en caso de desastre (DRP)	Única Vez	60 días naturales posterior a la integración de las mesas de trabajo
	Expedientes Curriculares del personal del SOC	Única Vez	15 días naturales posteriores a la notificación de adjudicación
Tablero De Estadísticas De Servicios De Seguridad (Portal Único)	Creación de cuentas de acceso en portal único de las soluciones de seguridad y red	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

11.2. Entregables Verificación Calidad

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades	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:	Evento	7 días hábiles posterior a la solicitud generada por parte del Instituto

ANEXOS
DIVISIÓN DE CONTRATOS

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	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	Evento	10 días hábiles posterior a la solicitud generada por parte del Instituto

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	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 posterior a la solicitud generada por parte del Instituto
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 posterior 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	Evento	5 días hábiles posterior a la solicitud generada por parte del

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	detalle de los dominios que se hayan renovados adquiridos.		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 posterior a la solicitud generada por parte del Instituto
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	Evento	10 días hábiles posterior 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 posterior 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 posterior al término de la implementación de cualquier solución de seguridad o conforme cada solicitud generada por el Instituto
	Actualización de la	Evento	5 días hábiles

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	matriz de escalación		posterior a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad
	Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad	Evento	5 días hábiles posterior a la ejecución de la ventana mantenimiento
	Reporte con Estadísticas de uso y desempeño (información analítica) de la soluciones de seguridad	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico de las configuraciones de las soluciones de seguridad	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico de los incidentes presentados en las soluciones de seguridad	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico de los requerimientos registrados en la mesa de servicios	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y su diagrama de	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	interrelación conforme fueron registrados en la CMDB		
	Diagramas de Arquitectura de las soluciones de seguridad	Evento	2 días hábiles posterior a la solicitud generada por parte del Instituto

11.3. Entregables Periódicos

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Seguridad – Continuidad Operativa	Reportes Técnicos de los activos de infraestructura que contemplen: • 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 posterior al cumplimiento del mes vencido
Servicios de Seguridad – Verificación/Calidad	Reportes Técnicos de los activos de infraestructura que contemplen: • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • Estadísticas de	Mensual	5 días hábiles posterior al cumplimiento del mes vencido

	uso de los servicios (conforme la definición en las mesas de trabajo)		
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 posterior al cumplimiento del mes vencido
	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posterior 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	Mensual	5 días hábiles posterior al cumplimiento del mes vencido

	realizadas en las mesas de trabajo		
	Reporte de las evaluaciones operativas a los servicios de seguridad implementados	Trimestral	5 días hábiles posterior 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 posterior al cumplimiento de cada trimestre calendario

El Proveedor deberá cumplir con los formatos provistos por el Instituto y en apego al Normatividad Vigente.

12. CONDICIONES DE ACEPTACIÓN

Se deberán formalizar los entregables descritos en el numeral anterior a efecto de dar por recibido los servicios requeridos.

Todos los documentos deben ser entregados en papel membretado de la empresa de manera impresa y en electrónico.

Se entregará a la División de Seguridad Informática Física perteneciente a la Coordinación de Telecomunicaciones y Seguridad de la Información.

13. 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.

14. CONVENIO DE CONFIDENCIALIDAD Y RESGUARDO DE LA INFORMACIÓN

El Proveedor de los **Servicios Administrados de Seguridad Informática Continuidad (SASI-C),** deberá suscribir el Convenio de Confidencialidad y Resguardo de Información correspondiente, en el que su representada o cualquiera de su personal asignado al proyecto por ningún motivo extraerán o divulgará el contenido de la información que se les entregará como parte del contrato.

Dicho documento debe ir firmada por su representante legal, en la que manifieste, que se compromete a respetar y seguir los estándares tecnológicos, tanto de metodologías, procedimientos, hardware, como de software definidos por el Instituto.

Asimismo, en dicha carta el proveedor deberá indicar que se compromete a que toda la información que exista a la fecha de la adjudicación y aquella que desarrolle derivado del presente proyecto será propiedad intelectual y exclusiva de "EL INSTITUTO" y no podrá ser utilizada por el proveedor para otros fines.

Por lo que deberá considerar al menos los siguientes mecanismos de control de acceso a la información del Instituto:

- Se deberán establecer controles de acceso y privilegios restringidos al personal del Proveedor del SASI-C, a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del Instituto.
- Se deberá implantar y aceptar en todo momento el uso de controles que permitan registrar "Pistas de Auditoria" para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.
- La seguridad lógica deberá estar protegida mediante el uso de dispositivos de control de acceso (Firewalls), mecanismos de encriptación y seguridad física entre las redes del Proveedor del SASI-C y las del Instituto.
- El almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por el proveedor de los servicios SASI-C, observando los requisitos de seguridad y resguardo de la información.
- El Proveedor del SASI-C deberá permitir el acceso a información relacionada con el servicio prestado al Instituto para la realización de auditorías.
- El Proveedor SASI-C 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.

15. 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.

16. MÉTODO DE EVALUACIÓN DE PROPUESTAS

Se evaluará mediante el criterio binario conforme a las características que presenten los proveedores en cuanto a funcionalidades en el Anexo Técnico como en el apéndice A del Anexo Técnico, con la finalidad de determinar la solvencia de las proposiciones a partir de verificar el cumplimiento de las condiciones legales, técnicas y económicas.

17. FUNCIONARIOS PÚBLICOS DE LA DIDT PARTICIPANTES EN EL PROCESO DE ADQUISICIÓN

a) C. Florencio Fernando González Velázquez, Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información.
b) C. Abraham Gutiérrez Castillo, Titular de la División de Seguridad Informática Física.
c) C. Cynthia Osmara Verdín Villegas, Jefe Área Nivel Central E0.

18. VIGENCIA DEL CONTRATO

La vigencia del contrato será a partir del día hábil siguiente a la notificación de la adjudicación y hasta el 31 de agosto de 2022.

19. PLAZO DEL SERVICIO

La prestación de los servicios iniciará a partir del día hábil siguiente al de la notificación de la adjudicación y hasta el 31 de agosto de 2022.

20. 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

21. MECANISMOS DE CONTROL PARA LA ADMINISTRACIÓN DEL CONTRATO

El Administrador del Contrato en conjunto con el Proveedor deberán generar el acta de entrega-recepción conforme a los entregables del Anexo Técnico.

22. MECANISMOS REQUERIDOS AL PROVEEDOR PARA RESPONDER POR DEFECTOS O VICIOS OCULTOS DE LOS BIENES O DE LA CALIDAD DE LOS SERVICIOS

No aplica

23. OTORGAMIENTO DE ANTICIPO

No aplica

24. FIRMAS DE FORMALIZACIÓN DEL DOCUMENTO

Elaboró
C. Cynthia Osmara Verdín Villegas Jefe Área Nivel Central E0.

Revisó
C. Abraham Gutiérrez Castillo Titular de la División de Seguridad Informática Física.

Aprobó
C. Florencio Fernando González Velázquez Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información.

IMSS	INSTITUTO MEXICANO DEL SEGURO SOCIAL DIRECCIÓN DE ADMINISTRACIÓN UNIDAD DE ADQUISICIONES COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS	Contrato Número S2M0038

ANEXO 2 (DOS)

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

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

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

INSTITUTO MEXICANO DEL SEGURO SOCIAL
IMSS

Investigación de Mercado para la contratación de los "Servicios Administrados de Seguridad Informática Continuidad (SASI-C)"

Propuesta Técnica

18/02/2022

Contenido

ANEXOS
DIVISIÓN DE CONTRATOS

TOTALSEC, S.A. DE C.V., manifiesta su interés en participar en la presente Investigación de Mercado y presenta su Afirmativo de propuesta técnica para los "**SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA CONTINUIDAD (SASI-C)**" que convoca **EL INSTITUTO MEXICANO DEL SEGURO SOCIAL (IMSS).**

Ciudad de México a 18 de febrero de 2022

ANEXO TÉCNICO
Especificaciones Técnicas

1. Objetivo

El **Instituto Mexicano del Seguro Social (IMSS)**, actualmente cuenta con un servicio administrado de seguridad integral, que provee la infraestructura de toda la gama de equipos de seguridad con los que se da atención a los servicios y a las aplicaciones propias del IMSS, por lo que con el propósito de mantener la continuidad de la operación del día a día del negocio, es indispensable contar con niveles de servicio de alta disponibilidad que garanticen la operación de la infraestructura de seguridad, almacenamiento, comunicaciones y respaldos, así como otros componentes habilitadores, que soportan los Servicios operativos institucionales, aplicando las mejores prácticas de TI y garantizando los niveles de servicio, calidad y oportunidad solicitados por el IMSS.

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 que garanticen la continuidad operativa, de negocios y de seguridad de la información del **Instituto**.

2. Beneficios

Los beneficios del Servicio de Seguridad Informática son los siguientes:

- Garantizar la continuidad operativa, la continuidad del negocio y la continuidad de la seguridad de la información en la Institución.
- Fortalecer la seguridad de la información de la Institución contra amenazas, disminuyendo el riesgo de sufrir incidentes de seguridad, mediante el uso de tecnologías de punta para el monitoreo, detección, aseguramiento, y contención de ataques que puedan presentarse en la infraestructura de cómputo, sistemas y aplicaciones propios del IMSS.
- Garantizar la confidencialidad de la información que el IMSS genera, recibe y procesa en su operación.
- Contar con servicios medidos por niveles de servicio, que migren, habiliten y mantengan a punto los componentes necesarios en los centros de datos del **Instituto** y que de forma complementaria gestionen operen, monitoreen, den soporte y mantenimiento preventivo y correctivo a la infraestructura, con el propósito de satisfacer las necesidades que se tienen en

cuanto a conectividad, comunicación, protección, control y filtrado de la propia Institución, manteniendo la plataforma tecnológica en condiciones óptimas de operación.

- Contar con servicios de seguridad de la información, que complementen el esquema de seguridad institucional de forma consistente y robusta, con el control, aseguramiento, diagnóstico, protección, pruebas, metodologías, de distintos rubros como el de acceso a cuentas privilegiadas, base de datos, aplicaciones, fuentes múltiples, vulnerabilidades, investigación forense y de procesos de seguridad, así como con otros servicios especializados en materia de seguridad y tecnologías de la información.
- Contar con personal calificado con la experiencia requerida para soportar todas y cada uno de los requerimientos del **Instituto**.

3. Alcance

TOTALSEC, S.A. DE C.V., establece las especificaciones y lineamientos técnicos para la prestación del Servicio de Seguridad Informática.

TOTALSEC, S.A. DE C.V., brinda a **El Instituto Servicios Administrados de Seguridad Informática Continuidad (SASI-C)**, con la finalidad de mantener, robustecer y complementar la seguridad institucional, centros de datos propios o de terceros en instalaciones del **Instituto**, o donde este lo requiera.

El proyecto abarca la toma de operación para las tecnologías funcionales de seguridad con las que cuenta hoy en día el **Instituto** como son: Firewalls, IPS, Filtrado de Contenido, Anti DDoS, Antispan, WAF, DBF, VPN, entre otras, la actualización tecnológica en *hardware* y *software* durante el período de transición.

Al término de la vigencia del contrato, **TOTALSEC, S.A. DE C.V.,** considera un periodo de **dos meses** para la transición a un nuevo proveedor de servicios, que se utilizaran para la entrega de toda la documentación técnica correspondiente al servicio que se encuentre en operación a la conclusión de los servicios y contar con el apoyo en todo momento para la transición.

4. Requerimientos del servicio

Los Servicios ofertados por **TOTALSEC, S.A. DE C.V.**, y que son parte de la solución propuesta incluyen al menos lo siguiente:

- **Servicios de Seguridad - Continuidad Operativa**

  Son los servicios de continuidad operativa para la seguridad perimetral que incluye los siguientes: (Firewalls, IPS, AntiDDoS, Filtrado Web, firewall de Aplicaciones WEB, Firewall de base de datos, cifrado de información, Control de Accesos, entre otros.), servicios que cumplen con los niveles de servicio establecidos para que de manera inmediata y en donde lo requiera el **Instituto** se continue con la operación. Estos servicios serán bajo demanda conforme a petición expresa del **Instituto**, así como los tiempos de entrega serán conforme al sitio y dependiendo del tipo de tecnología.

- **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, las pruebas de seguridad (revisiones de vulnerabilidades a los aplicativos web), cumplimiento normativo y herramientas de seguridad, así como los niveles de servicio requeridos la operación, incluyendo el soporte y resolución de problemas e incidentes.

- **Servicios del Centro de Operaciones de Seguridad (SOC)**

  El **Instituto** requiere que **TOTALSEC, S.A. DE C.V.**, mediante su Centro de Operaciones de Seguridad (SOC), que se encuentre físicamente en las instalaciones de **TOTALSEC, S.A. DE C.V.** El objetivo de este centro es brindar 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, 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 funcionamiento 7x24x365, etc.) El SOC de **TOTALSEC, S.A. DE C.V.**, se acredita con presentación de la copia simple del certificado ISO27001 vigente.

  Nota: Para validar el cumplimiento de los "Certificado ISO27001 vigente" referirse a **Anexo Certificados de Empresas**

5. Descripcion de los servicios

5.1. SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA

5.1.1. 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 **TOTALSEC, S.A. DE C.V.**, cumple con las siguientes especificaciones funcionales mínimas.

TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

Detalles del Servicio:

TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- Proporciona la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el **Instituto**, 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.
- Integra activos de infraestructura de propósito específico (Appliances) con capacidades de expansión bajo demanda, para la continuidad operativa del **Instituto**, conforme lo dispuesto en el Apéndice A.
- Definirá 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 los necesidades operativas de este.
- Llevará 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**.
- Acordará 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.
- Continuará 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.
- Garantiza 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.
- Permite 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.

- Continua 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**.
- Atenderá todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el **Instituto** genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- 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.
- Integra todo 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.
- Realizará evaluaciones operativas a los servicios, 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 derivados de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones serán ejecutadas al mes del inicio de operaciones de los servicios.
- Realizará todas aquellas 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.
- Proporciona al **Instituto** cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporciona 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.
- Cumple con las especificaciones técnicas y operativas descrita en el Apéndice A.

5.1.2. 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.

Detalles del Servicio:
TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el **Instituto**, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos a este servicio.
- 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/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.
- Permite 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 todo 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.
- 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 serán ejecutadas al mes del inicio de operaciones de los servicios.

- Realizar todas aquellas 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 todas aquellas 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 serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al **Instituto** cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumple, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice A.

5.1.3. Servicios de Protección contra Denegación de Servicio (DDoS)

Descripción del servicio:
El **Instituto** requiere de un servicio de protección contra ataques de Denegación de Servicio Distribuido que se encuentren basados en firmas y volúmenes de conexión altos.

Detalles del Servicio:

TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el **Instituto**, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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.
- Permite 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 todo 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.
- 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 serán ejecutadas al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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 serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al **Instituto** cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumple con las especificaciones técnicas y operativas descrita en el Apéndice A.

ANEXOS
DIVISIÓN DE CONTRATOS

5.1.4. Servicios de Redes Privadas Virtuales (VPN)

Descripción del servicio:
El **Instituto** requiere del Servicio de interconexión a través de Internet que permitan establecer comunicación desde localidades remotas para la transferencia de información a través de un canal cifrado.

Detalles del Servicio:
TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el **Instituto**, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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.
- Permite 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 todo 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.
- 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 serán ejecutadas al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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 serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al **Instituto** cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumple con las especificaciones técnicas y operativas descrita en el Apéndice A.

5.1.5. Servicios de Filtrado de Contenido Web

Descripción del servicio:

El **Instituto** requiere del servicio de filtrado de contenido Web mediante políticas de acceso que permita controlar y filtrar la utilización del servicio de acceso a Internet, en función de roles y perfiles.

Detalles del Servicio:

TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el **Instituto**, 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.

- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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 necesarios 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.
- Permite 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 todo 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.
- 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 serán ejecutadas al mes del inicio de operaciones de los servicios.

- Realizar todas aquellas 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 serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al **Instituto** cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumple con las especificaciones técnicas y operativas descrita en el Apéndice A.

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

Descripción del servicio:
El **Instituto** requiere de un servicio para analizar correos electrónicos de entrada y salida con el objetivo de bloquear aquellos que sean clasificados como spam, malware, phishing, entre otros.

Detalles del Servicio:
TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el **Instituto**, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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.
- Permite 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 provista a través del servicio.
- Integrar todo 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.
- 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 serán ejecutadas al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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 serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al **Instituto** cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumple con las especificaciones técnicas y operativas descrita en el Apéndice A.

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

Descripción del servicio:

El **Instituto** requiere del servicio de protección, prevención y control de ataques para aplicativos web expuestos en Internet/Intranet.

Detalles del Servicio:

TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el **Instituto**, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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 centralizado 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.
- Permite 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 todo 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.
- 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 nuevos funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones serán ejecutadas al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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 los mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al **Instituto** cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumple con las especificaciones técnicas y operativas descrita en el Apéndice A.

5.1.8. Servicios de Firewall de Base de Datos (DBF)

Descripción del servicio:

El **Instituto** requiere de un 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.

Detalles del Servicio:

TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el **Instituto**, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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.
- Permite 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 todo 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.
- 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 serán ejecutadas al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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 serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al **Instituto** cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumple con las especificaciones técnicas y operativas descrita en el Apéndice A.

5.1.9. Servicios de Gestión Unificada de Amenazas (UTM)

Descripción del servicio:

El **Instituto** requiere de un servicio de protección perimetral especializada en control de acceso, prevención de intrusos, filtrado de contenido Web y VPN, para control de tráfico y detección de actividad anómala.

Detalles del Servicio:

TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- Proporciona la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el **Instituto**, 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.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades 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.
- 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.
- Permite 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 todo 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.
- 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 serán ejecutadas al mes del inicio de operaciones de los servicios.
- Realizar todas aquellas 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 serán de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al **Instituto** cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumple con las especificaciones técnicas y operativas descrita en el Apéndice A.

5.2. SERVICIOS DE SEGURIDAD – VERIFICACIÓN/CALIDAD

El **Instituto** requiere continuar con la prestación de servicios bajo demanda durante la vigencia del contrato, que a través de este se definen, identifican, clasifican y priorizan las debilidades de los aplicaciones que proporcionen una evaluación de las amenazas previsibles y reaccionar de manera apropiada, así como robustecer la confidencialidad, integridad y disponibilidad de la información, atendiendo a las necesidades operativas del IMSS.

5.2.1. Servicios de Análisis de Vulnerabilidades

Descripción del servicio:
El **Instituto** requiere la continuidad operativa de un servicio que permita ejecutar análisis técnicos especializados sobre los activos en aplicaciones web e infraestructura, con la finalidad de identificar vulnerabilidades nuevas o conocidas.

Detalles del Servicio:
TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- Integra todas 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 solicitado.
- Da 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 permitan continuar con los servicios y activos de infraestructura que correspondan.
- Garantiza 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.
- Identifica los servicios a analizar, incluyendo el número de servidores involucrados y la versión de los 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.
- Integra un proceso y/o procedimiento para la continuidad de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada.
- Implementar una solución tecnológica que permita realizar pruebas de una manera centralizada y con soporte al menos a los siguientes lenguajes de programación: HTML, Java, .Net, C#, PHP.
- Integrar todo 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.
- 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**.
- Integrar las mejores prácticas de seguridad en el software mencionadas en el modelo de madurez propuesto y alineado OWASP.
- Realizará la transferencia de las prácticas de seguridad en el software implementadas al personal que el **Instituto** designe para dicho propósito.
- Preservar la integridad y confidencialidad de la información recibida durante la ejecución de las pruebas correspondientes.
- 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.

Nota: Para validar el cumplimiento de los "proceso y/o procedimiento" referirse al apartado "Anexos Generales" al final de este documento en la sección llamada "Metodologías".

- **TOTALSEC, S.A. DE C.V.,** integra 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.

Nota: Para validar el cumplimiento del "personal especializado" referirse al "Anexo Perfiles -totalsec"

5.2.2. Servicios de Pruebas de Penetración

Descripción del servicio:
El **Instituto** requiere la continuidad de un servicio que permite 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.

Detalles del Servicio:

TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- 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 solicitado.
- Dar seguimiento a los servicios o activos de información que son analizados, incluyendo el número de equipos involucrados, y la versión de las plataformas de los sistemas analizados.
- Identificación de vulnerabilidades y malas configuraciones.
- Explotación de acceso a los sistemas mediante el aprovechamiento de los huecos de seguridad detectados y/o vulnerabilidades detectadas.
- Evaluación de vulnerabilidades de al menos los siguientes rubros:
    - Autenticación y Autorización
        - Intentos ilimitados de inicio de sesión
        - Insuficiente autenticación
        - Insuficiente autorización
    - Gestión de sesión
        - Predicción de sesión

        - Secuestro de sesión
        - Reproducir sesión
        - Expiración de sesión insuficiente
    - Inyección de código
        - Inyección comando de Sistema Operativo
        - Inyección SQL
        - Cross-site Scripting
        - Inyección LDAP
        - Inyección HTML
        - Parameters Tampering
        - Cookie Poisoning
        - Hidden Field Manipulation
    - Criptografía
        - Fortaleza del algoritmo
        - Gestión de llaves
    - Ataques Lógicos
        - Abuso de funcionalidades
        - Input Field Validation Checking
    - Protección de Datos
        - Transporte
        - Almacenamiento
    - Divulgación de Información
        - Indexado de directorio
        - Path Traversal
        - Manejo inseguro de errores
        - Comentarios HTML
- Realizar un reporte ejecutivo y técnico, por cada requerimiento atendido, en el que se describan los detalles de los riesgos asociados a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP llamada "OWASP Risk Rating Methodology", detallando recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.
- Integrar un proceso y/o procedimiento para la continuidad de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada.

Nota: Para validar el cumplimiento de los "proceso y/o procedimiento" referirse al apartado "Anexos Generales" al final de este documento en la sección llamada "Metodologías".

- **TOTALSEC, S.A. DE C.V.**, integra 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.

Nota: Para validar el cumplimiento del "personal especializado" referirse al Anexo Perfiles -totalsec

5.2.3. Servicios de Analisis 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 identifican 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.

Detalles del Servicio:

TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

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

5.2.4. Servicios de Borrado Seguro de Información

Descripción del servicio:
Se requiere dar continuidad a la solución de borrado seguro de información, para los dispositivos como son 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 **TOTALSEC, S.A. DE C.V.**, así como las entregas de información requeridas en el presente documento, se apegan a la normativa vigente aplicable para dichos servicios y soluciones.

Detalles del Servicio:

TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- Integrar todas aquellas renovaciones que sean necesarios 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.
- Permite 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.
- Asegura 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.
- Brinda la destrucción local y/o remota en múltiples dispositivos de almacenamiento.
- Posibilita el desmontaje RAID (SCSI).
- Permite el borrado y detección de zonas bloqueadas / ocultas (DCO, HPA).
- Genera 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.
- Emite una firma electrónica para la autenticación de la integridad del reporte de sanitización emitido por el *software* de borrado.
- La solución se ejecuta sin importar de que sistema operativo se trate.
- El reporte que genera la solución puede 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 contempla entre otros, los siguientes puntos:
    - Solicitud de borrado.
    - Identificación del medio de borrado.
    - Definición de fecha de borrado.
    - Flujos operativos para la autorización de borrado o destrucción.

- Como referencia, se muestran los insumos a ser atendidos

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

- La continuidad del servicio considera 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).

5.2.5. Servicios de gestión de Dominios

Descripción del servicio:

Contar con un servicio que permita al **Instituto** poder registrar ante las instancias certificadas por el NIC, los dominios que requiera el **Instituto** y su correcta gestión.

Detalles del Servicio:

TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- 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

TOTALSEC, S.A. DE C.V., continuará con la gestión y pagos que correspondan derivados del registro, cambio de dominio o proveedor sin costo adicional para el **Instituto**.

5.2.6. 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.

Detalles del Servicio

El servicio de certificados digitales SSL que brinda **TOTALSEC, S.A. DE C.V.**, comprende lo siguiente:

- Validación de dominios
- Encripción SSL de al menos 256 bits
- No es auto firmado, sino emitido por instancia certificadora valida (tercero confiable)
- El tiempo de emisión es menor a 24 Horas y hacerlo llegar al personal del **Instituto.**
- **TOTALSEC, S.A. DE C.V.**, se hara cargo de la gestión en cuanto a pagos de derecho y cualquier cargo derivado de contar con el o los certificados.
- Los certificados son 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)

5.2.7. 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 esta basado en el estándar ISO 27001, 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 considera las actualizaciones que correspondan.

Detalles del Servicio:

TOTALSEC, S.A. DE C.V., garantiza la continuidad operativa de este servicio y cumple con al menos las siguientes funcionalidades operativas:

Planear

- Capacitación de seguimiento – Curso "Inducción a la norma 27001:2013 o vigente.
  Curso que permita al participante:
    - 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 considera 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 se apega a lo siguiente:
  - Dominios que establece la norma ISO 27001.
  - 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 considera 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 considera los siguientes temas:
  - Identificación y aplicabilidad de los requerimientos internos y externos
  - Selección de los objetivos de control y controles para el tratamiento de los riesgos
  - Verificación de requerimientos contractuales y legales
  - Identificación de los requerimientos internos y externos
  - Validación de aplicabilidad de los requerimientos
  - Formato de Autorización para implantar y operar el Sistema de Gestión de Seguridad de la Información
  - Preparación de la declaración de aplicabilidad
  - Documentar los objetivos de control y los controles elegidos y la justificación de su elección
  - Documentar los controles actualmente implementados
  - Documentar la exclusión de controles y la justificación de su exclusión
- Operación el Sistema de Gestión de Seguridad de la Información
  - Análisis de Riesgos de Seguridad de la Información
  - Análisis de riesgo con base en lo definido en el servicio de gestión de riesgos de seguridad
  - Generación de la actualización del plan de tratamiento de riesgos
    La metodología considera los siguientes temas:
  - Identificación de las acciones a realizar por parte de la institución y su administración
  - Identificación de los recursos necesarios y prioridades
  - Identificación de las responsabilidades para administrar los riesgos de seguridad de la información
- Aplicación del seguimiento al plan de tratamiento de riesgos.
  La metodología considera 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

ANEXOS
DIVISIÓN DE CONTRATOS

- Definición del proceso de reporte y atención de incidentes de seguridad
- Propuestas de implementación de los controles seleccionados.
  La metodología considera 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 dentro definido en el alcance.
- Administración del cambio cultural.
  La metodología considera los siguientes temas:
  - Actualización del Programa de concientización con usuarios y operadores del Sistema de Gestión de Seguridad de la Información
  - Seguimiento y apoyo a las necesidades de capacitación para el personal que administra el Sistema de Gestión de Seguridad de la Información y seguridad de la información
  - Manual de Gestión de Seguridad de la Información.
    Se documentará un manual que contenga las referencias generadas en esta fase para dar trazabilidad al de las cláusulas de la norma.
- Monitorear y Revisar el Sistema de Gestión de Seguridad de la Información
  Revisiones gerenciales.
  La metodología considera los siguientes temas:
  - Los dueños del proceso harán una revisión y actualización al Sistema de Gestión de Seguridad de la Información con la finalidad de verificar que los objetivos del Sistema de Gestión de Seguridad de la Información están alineados a los objetivos de negocio en materia de seguridad de la información y que garantizan el adecuado manejo de los riesgos existentes.
  - **TOTALSEC, S.A. DE C.V.**, actualiza el procedimiento de revisiones gerenciales.
  - **TOTALSEC, S.A. DE C.V.**, actualizará los formatos requeridos para llevar a cabo las revisiones gerenciales
- Auditorías internas.
  La metodología considera lo siguiente:
  - Seguimiento y apoyo en la generación del plan de auditorías internas a las áreas de TI y a los terceros que proveen servicios de TI al **Instituto**.
  - Actualización o en su caso definición de los formatos requeridos para llevar a cabo las auditorías
  - Aplicación de una auditoría interna al Sistema de Gestión de Seguridad de la Información para verificar el cumplimiento con el estándar ISO/IEC 27001:2013 o vigente y a los procesos establecidos en la normativa vigente aplicable.
- Actualización del Sistema de Gestión de Seguridad de la Información
  Implementación de mejoras
  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.
  Considera lo siguiente:
  - Apoyo en la definición y seguimiento del procedimiento para realizar acciones correctivas y no conformidades derivadas de las auditorias.
  - Actualización del formato para llenado de acciones correctivas y no conformidades.
  - Coordinación de la ejecución de las acciones correctivas ya definidas y en su caso las no conformidades que se identifiquen.
- Comunicar los resultados de las acciones tomadas.
  Se considera 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**.

Nota: Para ver a detalle el proceso de"SGSI" referirse al apartado "Anexos Generales" al final de este documento en la sección llamada "Metodologías".

5.3. SERVICIOS DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

El **Instituto** requiere que el proveedor del servicio cuente con un Centro de Operaciones de la Seguridad (SOC), que se encuentre físicamente en las instalaciones del proveedor. El objetivo de este centro es ser la continuidad operativa a la gestión de la seguridad, así como responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad, que ejecute actividades de revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, análisis forense, notificación de alertas y vulnerabilidades, así como el establecimiento de acciones de mejora sustentable.

TOTALSEC, S.A. DE C.V., considera que el servicio de SOC se refiere a las soluciones propuestas e implementadas hoy en día por el **Instituto**, así mismo considera que la correlación de bitácoras se basa en un servicio de correlación de eventos e incidentes de seguridad en el que los casos de uso son ilimitados, así como las respuestas ante un incidente alineadas a tiempo de los niveles de servicio (SLA) establecidos para este servicio.

Nota: Para ver a detalle los procesos de"SOC" referirse al apartado "Anexos Generales" al final de este documento en la sección llamada "Metodologías".

Detalles del Servicio:

TOTALSEC, S.A. DE C.V., brinda el presente servicio conforme lo siguiente:

- Se Ubica dentro de territorio nacional.

- Operación continua las 24 horas del día, los 7 días de la semana y durante los 365 días del año (7x24x365), esto último conforme la vigencia del contrato.
- Cuenta con personal para la atención del servicio en sitio y de forma remota, el cual es personal calificado con base en las credenciales requeridas para la administración y monitoreo de los componentes que integran la solución.
- Operación en un centro de datos alterno ubicado dentro de territorio nacional.
- Mantenimiento de las suscripciones a sitios y listas de empresas, fabricantes y medios especializados en seguridad de la información, que permitan alertar sobre nuevas vulnerabilidades.
- Infraestructura dedicada para la administración, operación y monitoreo de los componentes *hardware* y *software* que componen los servicios de seguridad.
- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones se ejecutarán cada 3 meses, desde el inicio de operaciones de los servicios y hasta 1 mes antes del término de estos.
- Realizar acciones correctivas y preventivas para asegurar la confidencialidad, integridad y disponibilidad de la información que se maneja en las diferentes soluciones se seguridad.
- Notificaciones y alertas personalizadas, en caso de desviaciones, anormalidades o brechas de seguridad, para cada una de las soluciones de seguridad.
- Revisiones continuas a la operación del SOC, que permitan establecer mejora en los procesos, procedimientos y controles de seguridad.
- Analizar los eventos de seguridad y administración de bitácoras que se integran en los servicios de correlación de información, a fin de establecer acciones preventivas a través de modificaciones a las configuraciones de las soluciones de seguridad.
- Integra un Equipo de Atención y Respuesta a Incidentes de Seguridad.
- Soporte y Atención a fallas a los componentes hardware y software que integran la solución, conforme los estipulado en los acuerdos de niveles de servicio.
- Monitorear la disponibilidad de los componentes hardware y software que integran la solución ofertada. La solución de monitoreo tiene 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:
    - Administración de Dispositivos.
    - Administración de Requerimientos.
    - Administración de Cambios.
    - Administración de Configuraciones.
    - Administración de Vulnerabilidades.
    - Administración de Incidentes.
    - Administración de Problemas.
- Integración de una Mesa de servicio apegada a ITIL v4, la cual se 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 permiten 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, permite la generación de eventos (tickets), mediante los mecanismos que se establezcan en las mesas de trabajo correspondiente, que, de manera enunciativa más no limitativa, pueden ser:
  - Un número telefónico directo en las instalaciones del SOC.
  - Un número telefónico a diez dígitos.
  - Correo Electrónico
  - Portal Web
- El personal de **TOTALSEC, S.A. DE C.V.**, que atenderá las operaciones de los servicios de seguridad, cuenta con experiencia probada en las áreas de tecnología y de seguridad de la información previamente mencionadas, para lo cual, se integra el currículo vitae de todo el personal que participe en el servicio, indicando al menos:
  - Experiencia profesional: bajo este rubro, se considerarán todos los puestos que cada integrante haya desempeñado, con fecha, nombre de los empleadores, nombre de los puestos que ha ejercido y el tipo de funciones bajo su responsabilidad, y cuenta con experiencia comprobable al menos 5 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 cuenta con experiencia comprobable de al menos 5 años.
  - Estudios: bajo este rubro se anotarán todos los estudios en materia de seguridad de la información, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica. Las certificaciones son de tecnología y/o de seguridad de tipo "vendor-neutral".
  - Incluir la estructura del grupo de trabajo, indicando por cada perfil las responsabilidades y competencias.
- El **Instituto** podrá solicitar la revisión de la infraestructura de seguridad por un tercero en cualquier momento, durante la vigencia del contrato, con la finalidad de dar certeza de la entrega del servicio.
- Seguimiento a la Base de Datos de la Gestión de la Configuración (CMDB por sus siglas en ingles) que contenga los detalles relevantes de cada elemento de configuración (CI) y de la relación entre ellos, incluyendo el equipo físico, software y la relación entre incidencias, problemas, cambios y otros datos del servicio de seguridad.
- Generar los reportes de Inteligencia de Negocio y Analítica de Información que permitan tener estadísticas del uso y desempeño de los servicios de seguridad, esto último con el objetivo de coadyuvar a la toma de decisión estratégica y operativa de los servicios, así como para determinar el plan de capacidad de cada tecnología implementada. Dichos reportes podrán considerar, de manera enunciativa más no limitativa, la siguiente información:
  - Estadísticas de uso de procesamiento por tecnología
  - Estadísticas de desempeño por tecnología (throughput)
  - Estadísticas de ataques informáticos bloqueados.
  - Estadísticas de comportamientos tipo esperado de uso por tecnología (líneas base)
  - Estadísticas de usuarios concurrentes por servicio.
  - Estadísticas de crecimiento diario, mensual y anual por cada servicio.
- Proporcionar al **Instituto** cuentas de acceso a las consolas de administración de los servicios de seguridad, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales son

de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.

- La consola de administración provistas para los servicios de seguridad permite visualizar al menos:
  - Políticas: Control de Acceso
  - Configuraciones: Listas de Control de Acceso (Listas Blancas, Listas negras), Líneas base de seguridad.
  - Objetos: Usuarios, Grupos, Direcciones IP
  - Bitácoras.
  - Estadísticas en tiempo real: Desempeño, procesamiento, usuarios conectados, conexiones por segundo, ancho de banda utilizado.
- Proporcionar al **Instituto** cuentas de acceso a las bases de conocimiento de las tecnologías integradas para cada solución o servicio, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso de los servicios de seguridad.
- Integrar un Tablero de Estadísticas de Servicios de Seguridad a través de un portal único de administración de los servicios de seguridad de forma independiente a los 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, **TOTALSEC, S.A. DE C.V.**, incluye en su oferta económica los costos asociados al desarrollo para el cumplimiento de éste requerimiento.
- Permite 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.

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

PERFIL	CERTIFICACIONES A DEMOSTRAR	EXPERIENCIA A DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Administrador del Centro de Operaciones de Seguridad (SOC)	CISM (Certified Information Security Manager) o CISSP (Certified Information Systems Security Professional)	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 recurso

PERFIL	CERTIFICACIONES A DEMOSTRAR	EXPERIENCIA A DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
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.	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 recursos
Analista de Seguridad	CEH (Certified Ethical Hacker)	3 años de experiencia en participación de proyectos de seguridad de la información.	Encargado de ejecutar las revisiones de seguridad sobre las aplicaciones y la infraestructura, así como prever, detectar, analizar, contener, erradicar, documentar incidente de seguridad.	Al menos 2
Líder de proyecto	PMP (Project Manager Professional) Certificado por PMI o ITIL v4 (Expert o Master)	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	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
Consultor de Penetración	GPEN (GIAC Certified Penetration Tester) o CEH (Certified Ethical Hacker) o CICP (Core Impact Certified Profesional)	3 años de experiencia en participación de proyectos de seguridad de la información.	Realiza 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 recurso

PERFIL	CERTIFICACIONES A DEMOSTRAR	EXPERIENCIA A DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Consultor Forense de Cómputo	EnCE (EnCase Certified Examiner) o CHFI (Certified Hacker Forensics Investigator)	3 años de experiencia en participación de proyectos de seguridad de la información.	Analiza, 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 recurso
Arquitecto Especializado en Redes y Seguridad	CCNP (Cisco Certified Network Professional) o CCSP	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 recurso

Nota: Para validar el cumplimiento de los "Perfiles" referirse al Anexo Perfiles -totalsec

6. 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 **TOTALSEC, S.A. DE C.V.**, efectuará bajo la supervisión de los funcionarios designados por este último para tales efectos.

6.1. 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 **TOTALSEC, S.A. DE C.V.**, efectuará bajo la supervisión de los funcionarios designados por este último para tales efectos.

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto	Única Vez	15 días naturales posterior a la notificación de adjudicación
	Documento Compromiso de suscripción del acuerdo de niveles operacional (*Operational Level Agreement*, OLA	Única Vez	15 días naturales posterior a la notificación de adjudicación
	Matriz de Escalación	Única Vez	15 días naturales posterior a la notificación de adjudicación
	Escrito por parte de **TOTALSEC, S.A. DE C.V.**, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	Única Vez	15 días naturales posterior a la notificación de adjudicación
Servicios de Seguridad – Continuidad Operativa	Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar en los	Única Vez	5 días hábiles posteriores a la integración de las mesas de trabajo por

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	centros de datos o donde lo indique el **Instituto**		cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el **Instituto**	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el **Instituto**, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las 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	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Implementadas, que requieran integran activos de infraestructura para su habilitación		componentes en los Centro de Datos o donde lo indique el **Instituto**, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad, que requieran integran activos de infraestructura para su habilitación	Única Vez	20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados
Servicios de Análisis de Vulnerabilidades	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Pruebas de Penetración	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Análisis Forense	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Borrado Seguro de Información	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicio de Gestión de Dominios	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicio de Certificados Digitales SSL	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior 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 posterior 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 posterior a la integración de las mesas de trabajo
Servicios del Centro de Operaciones de Seguridad (SOC)	Procesos de operación implementados: • Requerimientos • Cambios	Única Vez	15 días naturales posterior a la emisión del fallo

ANEXOS
DIVISIÓN DE CONTRATOS

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	• Configuraciones • Incidentes • Problemas • Monitoreo		
	Matriz de Escalación Técnica y Organizacional	Única Vez	15 días naturales posterior a la emisión del fallo
	Procedimiento de operación de la Mesa de Servicios: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	Única Vez	15 días naturales posterior a la emisión del fallo
	Plan de Recuperación en caso de desastre (DRP)	Única Vez	60 días naturales posterior a la integración de las mesas de trabajo
	Expedientes Curriculares del personal del SOC	Única Vez	15 días naturales posterior 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

6.2. Entregables bajo demanda

TOTALSEC, S.A. DE C.V., de manera enunciativa más no limitativa, generará entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades	Reporte Técnico y Ejecutivo en formato electrónica (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al	Evento	10 días hábiles posterior a la solicitud generada por parte del **Instituto**

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	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 para el proceso de análisis	Evento	10 días hábiles posterior a la solicitud generado 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 de activos de infraestructura verificados	Evento	15 días hábiles posterior a la solicitud generada por parte del **Instituto**
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	Evento	5 días hábiles posterior a la solicitud generada por parte del **Instituto**

ANEXOS

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado.		
Servicio de Gestión de Dominios	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos.	Evento	5 días hábiles posterior 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 posterior a la solicitud generada por parte del **Instituto**
Servicios de Sistema de Gestión de Seguridad de la Información	Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo	Evento	10 días hábiles posterior 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 posterior 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 posterior 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 posterior 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 posterior a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad y Red

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad y red	Evento	5 días hábiles posterior 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 posterior 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 posterior a la solicitud generada por parte del **Instituto**
	Reporte Técnico de los requerimientos registrados en la mesa de servicios	Evento	5 días hábiles posterior 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 posterior a la solicitud generada por parte del **Instituto**
	Diagramas de Arquitectura de las soluciones de seguridad y red	Evento	2 días hábiles posterior a la solicitud generada por parte del **Instituto**

6.3. Entregables Periódicos

TOTALSEC, S.A. DE C.V., de manera enunciativa más no limitativa, generará entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Seguridad – Continuidad Operativa	Reportes Técnicos de los activos de infraestructura que contemplen: • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa	Mensual	5 días hábiles posterior al cumplimiento del mes vencido

	• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)		
Servicios de Seguridad – Verificación/Calidad	Reportes Técnicos de los activos de infraestructura que contemplen: • 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 posterior 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 posterior al cumplimiento del mes vencido
	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posterior 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 posterior al cumplimiento del mes vencido
	Reporte de las evaluaciones operativas a los servicios de seguridad implementados	Trimestral	5 días hábiles posterior 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 posterior 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, **TOTALSEC, S.A. DE C.V.**, establecerá un repositorio digital, que, de manera alterna, servirá para alojar los entregables antes señalados, mismos que estarán disponibles para su consulta durante la vigencia del contrato, teniendo en cuenta que el **Instituto** definirá en las mesas de trabajo los permisos de acceso correspondientes para el administrador del contrato, cuerpo de gobierno que se conforme para este propósito u otros funcionaros que sean designados por el primero mencionado.

7. NIVELES DE SERVICIOS

Los Niveles de Servicio, así como penas convencionales y deducciones, se aplicarán conforme a lo estipulado en el documento denominado "Términos y Condiciones".

8. CONVENIO DE CONFIDENCIALIDAD Y RESGUARDO DE LA INFORMACION

TOTALSEC, S.A. DE C.V., actualizará y firmará el Convenio de Confidencialidad y Resguardo de Información correspondiente. Así mismo, considera al menos los siguientes mecanismos de control de acceso a la información del **Instituto**:

- Se establece controles de acceso y privilegios restringidos al personal de **TOTALSEC, S.A. DE C.V.**, con el fin de reservar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del **Instituto**.
- Se implanta y acepta en todo momento el uso de controles que permitan registrar "Pistas de Auditoria" para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.
- La seguridad lógica estará protegida mediante el uso de dispositivos de control de acceso (Firewalls), mecanismos de encriptación y seguridad física entre las redes de **TOTALSEC, S.A. DE C.V.**, y las del **Instituto**.
- Los empleados de **TOTALSEC, S.A. DE C.V.**, con acceso a la información sensible del **Instituto**, se firmarán acuerdos de confidencialidad con este último.
- El almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por **TOTALSEC, S.A. DE C.V.**, observando los requisitos de seguridad y resguardo de la información.
- **TOTALSEC, S.A. DE C.V.**, permitirá el acceso a información relacionada con el servicio prestado al **Instituto** para la realización de auditorías.
- **TOTALSEC, S.A. DE C.V.**, no hara 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.

9. NORMATIVIDAD APLICABLE

TOTALSEC, S.A. DE C.V., se sujetará a las políticas internas vigentes del **Instituto** y a cualquier modificación o inclusión de nuevas políticas que se realice durante la vigencia del contrato. Las políticas aplicables se le darán a conocer durante las mesas de trabajo, sin embargo, se consideran las que se enlistan a continuación, de manera enunciativa más no limitativa:

ANEXOS
DIVISIÓN DE CONTRATOS

- El 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.**
- Normas ISO/IEC27001:2013 o vigente (Copia simple a nombre de **TOTALSEC, S.A. DE C.V.**)

Nota: Para validar el cumplimiento de los "Certificados de Empresa" referirse al Anexo Certificados de Empresas

9.1. Cumplimiento de Políticas

TOTALSEC, S.A. DE C.V., respeta todas las políticas de seguridad vigentes en el **Instituto** y en ninguna circunstancia permite que se viole ninguno de los lineamientos vigentes. Si alguno de los lineamientos de Seguridad implantados en el **Instituto** llegase a cambiar en el transcurso del contrato establecido con **TOTALSEC, S.A. DE C.V.**, éste seasegurará de modificar su infraestructura y procesos de tal forma que cumpla con los nuevos requerimientos.

Todos los equipos de cómputo personal propiedad de **TOTALSEC, S.A. DE C.V.**, 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 "Troyanos". Esta regla aplica tanto para los equipos de cómputo móviles (laptops, handheld, smartphones, tablet PC, etc.) como para los equipos de escritorio (desktop, deskside, etc.) usados por los recursos designados para las diversas tareas de administración y gestión.

Si dichos equipos requirieran de la instalación de sistemas operativos, aplicaciones, sistemas antivirus, sistemas de seguridad y demás herramientas que **TOTALSEC, S.A. DE C.V.**, decida necesario para la correcta operación de su personal, así como de la adquisición, instalación, mantenimiento y licenciamiento de estos, el costo será absorbido por **TOTALSEC, S.A. DE C.V.**

9.2. Consideraciones en la finalización del Contrato

La infraestructura, los componentes habilitadores y los demás elementos utilizados por **TOTALSEC, S.A. DE C.V.**, se transferirán al IMSS para la continuidad operativa. Este acto se llevará a cabo mediante un acta de entrega recepción, en la que dichos componentes se transmitirán al IMSS, a título gratuito, libres de toda limitación de dominio, gravamen y responsabilidad de cualquier naturaleza, conforme a la normativa aplicable al **Instituto.**

TOTALSEC, S.A. DE C.V., entregará al **Instituto**, a más tardar 6 meses antes de la finalización del Contrato, un plan de trabajo detallado para lograr una transición efectiva, en el que se incluyan todos los hitos y plazos necesarios para efectuarlo. Dicho plan permite una completa y correcta transición de los servicios, incluyendo la conformación y actualización de la documentación necesaria del proyecto.

En el caso de celebrarse un convenio modificatorio que amplíe el tiempo originalmente pactado, el **TOTALSEC, S.A. DE C.V.**, acordar mediante mesa de trabajo con el administrador del contrato, el plazo en que habrá de llevarse a cabo esta actividad.

La documentación incluye 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 **Instituto** solicite se mantengan para la transición de un nuevo contrato de servicios, procurando afectar de forma mínima la operación.

TOTALSEC, S.A. DE C.V., garantiza los Niveles de Servicio durante transición a un nuevo proveedor. 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 **TOTALSEC, S.A. DE C.V.**, haya presentado previamente, y que el **Instituto** hubiera aprobado. No obstante, durante dicho periodo, **TOTALSEC, S.A. DE C.V.**, proporcionará la orientación tecnológica adecuada al personal del **Instituto** para garantizar la continuidad de los servicios requeridos, poniendo a disposición de un tercero la transferencia o quien el **Instituto** designe para dicho propósito.

9.3. Consideraciones posteriores al termino del Contrato

Una vez terminado la vigencia del servicio, la infraestructura, los componentes habilitadores y los demás elementos utilizados por **TOTALSEC, S.A. DE C.V.**, 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**.

10. PERFIL DE TOTALSEC, S.A. DE C.V.

TOTALSEC, S.A. DE C.V., cuenta 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.
Nota:-Para validar el cumplimiento de los "Certificados de Empresa" referirse al Anexo Certificados de Empresas.

11. CLAVE CUCoP

31904

12. REQUERIMIENTOS DE ARQUITECTURA TECNOLÓGICA

No Aplica

13. RESTRICCIONES E INTERFACES CON OTROS ELEMENTOS

No Aplica

14. UNIDAD DE MEDIDA

Servicios

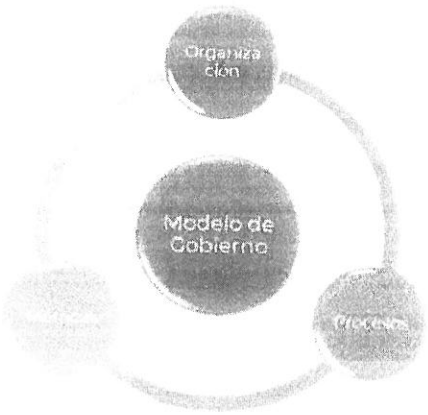
15. UNIDAD DE MEDIDA

El Modelo de Gobierno establece la forma como se trabajará en relación con este proyecto, los lineamientos operacionales para **TOTALSEC, S.A. DE C.V.**, y la manera como se medirá el grado de desempeño. El Modelo de Gobierno surge de la necesidad de diseñar una estructura operativa orientada a procesos para administrar los "Servicios Administrados de Seguridad Informática Continuidad (SASI-C)", 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 a fin de en cada una de las etapas del servicio, el del Administrador del Contrato y los Líderes del proyecto, con apoyo por parte de **TOTALSEC, S.A. DE C.V.**, del servicio (SOC), aseguren los niveles de servicios establecidos para la operación.



La estructura organizacional que ejecutar para el proyecto de "Servicios Administrados de Seguridad Informática Continuidad (SASI-C)", 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 deducciones 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".

Página 49

ANEXOS
DIVISIÓN DE CONTRATOS

totalsec
Expertos en Ciberseguridad

APÉNDICE A DEL ANEXO TÉCNICO

Investigación de Mercado para la contratación de los "Servicios Administrados de Seguridad Informática Continuidad (SASI-C)"

1. Servicio de Firewall

Para el "Servicio de Firewall", **TOTALSEC, S.A. DE C.V.**, considera un sistema de seguridad informática perimetral, el cual tiene como su principal función proteger y filtrar los riesgos de seguridad de la totalidad del tráfico entrante y saliente de Internet y de la red interna de el "IMSS", a través de este componente se configuran las políticas de operación para establecer los servicios permitidos con base en puertos lógicos y aplicaciones, además se realizará la configuración de las áreas denominadas Zonas Desmilitarizadas (DMZ) para la protección de servicios que requieran publicación a internet por parte del "IMSS", así como el manejo de alta densidad.

TOTALSEC, S.A. DE C.V., brinda al **IMSS**, en el presente estudio de mercado los siguientes componentes para el cumplimiento del requerimiento que se describe en las especificaciones técnicas:

Componentes Servicios de Firewall					
No	**Modelo**	**Características**	**Tipo**	**Cantidad**	**Sitio**
1	FortiGate-1800F	4 x 40GE QSFP+ slots, 12 x 25GE SFP28 /10GE SFP+ slots, 2x10GE SFP+ HA slots, 8 x GE SFP slots, 18 x GE RJ45 ports, SPU NP7 and CP9 accelerated, dual AC power supplies	3	2	Centro Médico Nacional de Occidente

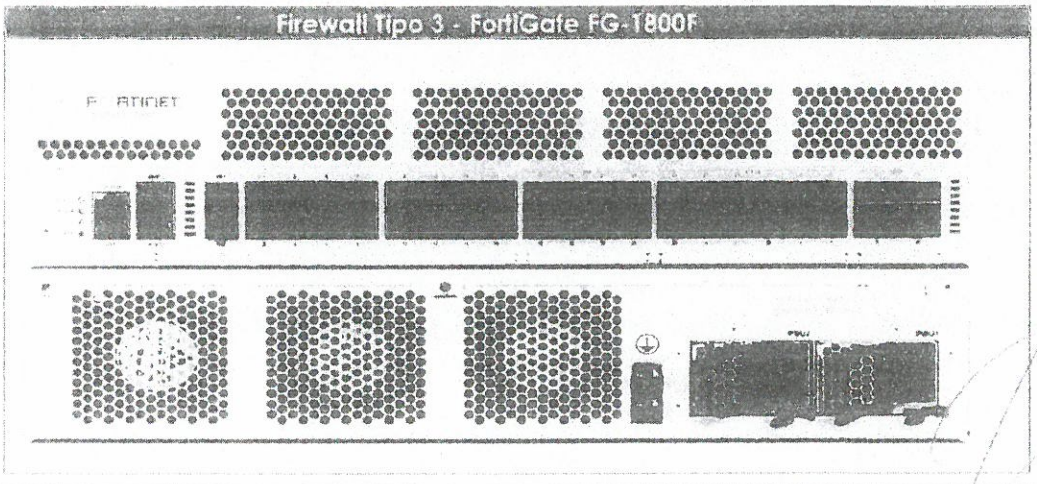
Tabla 1. Sericio de Firewall propuesto en alta disponibilidad

Por lo cual **TOTALSEC, S.A. DE C.V.**, proporcionará en el sitio Centro Médico Nacional de Occidente, un sistema de seguridad informática perimetral, la cual está compuesta por (2) equipos del fabricante Fortinet modelo FG-1800F en un esquema de alta disponibilidad, estos equipos están dimensionados para soportar lo solicitado por el IMSS con base a las especificaciones técnicas descritas en el "Apendice A Formato SASI-C v20122021".

En la siguiente tabla, se brindan las especificaciones técnicas que componen a estos equipos encargados de la seguridad perimetral y se muestran en los siguientes puntos:

- Se brindan 2 equipos tipo 3 para el Centro Médico Nacional de Occidente (configuración en HA

Firewall Tipo 3 - FortiGate FG-1800F



Características	Cantidad
Cantidad	2 Equipos
Ubicación	Filtrado Web (IPCyT)
Modelo	FG-1800F
Alta Disponibilidad	Activo/Pasivo o Activo/Activo
Troughput Firewall	198 Gbps
Sesiones Máximas	12 Millones
Nuevas Sesiones por Segundo	750,000
Interfaces de red	16 Interfaces Cobre 1G RJ45 Ethernet 6 Interfaces a 1 Gb Fibra SFP 12 Interfaces a 10 Gb Fibra SFP+ 4 Interfaces a 40 Gb Fibra QSFP+
Interfaz de Administración	2 Interfaz Cobre 1G RJ45 Ethernet
Fuente de Poder	Redundante
Dimensiones	2 Unidades de Rack
Máximo BTU/hr	1906.70
Fuente de Alimentación	558.8 W
Voltaje de Entrada	AC: 100-240 VAC (50/60 Hz)

Tabla 2. Especificaciones técnicas de equipo FG-1800F.

Los equipos Fortinet modelos FG-1800F propuestos por **TOTALSEC, S.A. DE C.V.**, cuentan con la funcionalidad de FIREWALL, la cual se describe a continuación:

Funcionalidad	Descripción
Firewall **FW**	El **Firewall** de FortiGate brinda las siguientes capacidades en la seguridad perimetral: o Proteger de accesos no autorizados dentro de la red, a través de permitir o denegar la comunicación con diferentes puertos o servicios. o Realiza traducciones de direcciones de red, permitiendo el enmascaramiento de la dirección IP interna que realiza la petición.

Tabla 3. Funcionalidad de Firewall.

TOTALSEC, S.A. DE C.V., considera el hardware, soporte, conectores necesarios para la instalación, y el personal necesario para llevar a cabo la preparación, planificación, el diseño, implementación operación y administración de los equipos **Firewall** solicitados durante la vigencia del contrato.

Especificaciones Técnicas:

- **TOTALSEC, S.A. DE C.V.**, 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

Tabla 4. Especificaciones técnicas de "Tipos de Firewall".

Se brindan 2 equipos tipo 3 para el Centro Médico Nacional de Occidente (configuración en HA)

TOTALSEC, S.A. DE C.V., proporciona la continuidad del servicio conforme a lo siguiente:

- Considera características de conexiones simultaneas por segundo, es decir conexiones concurrentes por segundo.
- Continuidad y seguimiento del sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Esta basado en tecnología conocida como "Stateful Inspection", la 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.
- Este certificado por organismos de la industria como Common Criteria o ICSA Labs.
- Crea NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permite implementar reglas aplicadas a intervalos de tiempo específicos.
- Integra listas de control de acceso basadas en dirección origen, dirección destino, protocolos, interfaces de red, puertos, URL destino, identidad, rangos de tiempo o periodo.
- Tiene la capacidad de agrupar objetos tales como direcciones IP, protocolos y puertos para la simplificación de configuración de políticas de seguridad.
- Tiene la capacidad de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con tiempo de espera agotado (timeout).
- Tiene la capacidad de continuar con los 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).
- Cuenta con la capacidad de inspeccionar tráfico FTP, HTTP, HTTPS, DNS, ICMP, RADIUS, SMTP y SNMP, H.323, SIP, RSTP, SNMP, entre otros.
- Cuenta con la capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Soporta alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Cuenta con la 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.
- 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).
- Cuenta con la capacidad para ser integrado con servicios de correlación de eventos de seguridad.
- Soporta y opera bajo protocolos de ruteo BGP y OSPF.
- Soporta y opera mediante rutas estáticas.
- Realiza inspección en capa 3 y 4.

- Soporte y operación con al menos 1,000 VLANs
- Integra esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Almacena una base de usuarios local que permite realizar autenticación, sin depender de un dispositivo externo.
- Cuenta y opera al menos con una interfaz Gigabit Ethernet dedicada para administración.
- Generación de bitácoras de eventos (logs) con múltiples niveles de criticidad.
- Da continuidad y opera la consola centralizada de gestión que cuenta 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, es capaz de regresar a la configuración anterior, si es necesario o requerido.
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, que incluya al menos el 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 incluye fecha y hora de cada actividad realizada.

2. Servicio de Prevención de Intrusos (IPS)

Para el "Servicio de Prevención de Intrusos (IPS)", **TOTALSEC, S.A. DE C.V.**, considera una protección perimetral basado en firmas e identifica vulnerabilidades, para contener los intentos de obtener acceso a los recursos o servicios publicados en Internet o Intranet que pudieran afectar la operación de la organización, detectar accesos no autorizados y prevenir fugas de información.

Especificaciones Técnicas:

TOTALSEC, S.A. DE C.V., proporciona la continuidad del servicio conforme a lo siguiente:

- Continuidad y seguimiento del 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 operan en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
- Es 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 alerta que eventos serán 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 contempla 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 es 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.
- Es capaz de soportar análisis de tráfico de voz sobre IP.
- Es capaz de soportar monitoreo de VLANs, incluyendo tramas 802.1q
- Es capaz de soportar monitoreo de IPv6.
- Soporte de monitoreo con inspección profunda de paquete y monitoreo de paquete en escenarios de alta disponibilidad y con handshake TCP incompleto.
- Reconocimiento de tuneleo de protocolos que permite la identificación de protocolos aun cuando estos estén encapsulados.
- Detección de escaneo de puertos.
- Detección de reensamblaje 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 puede ser usado para hacer reconstrucción o análisis forense del ataque.
- Integración de listas blancas (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.
- Cuenta con la capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Cuenta con la 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.
- Cuenta con la capacidad de integración con el directorio de usuarios (Active Directory y/o LDAP).
- Cuenta con la 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.
- Continuidad y administración de la consola centralizada que administre los IPS y la integración de usuarios que realice las configuraciones necesarias para remediación de incidentes de seguridad.
- Continuidad y administración de la 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

ANEXOS
DIVISIÓN DE CONTRATOS

afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que incluyo fecha y hora de cada actividad realizada.

- Soporta 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.
- Continuidad y administración de la consola para los equipos en el centro de datos, principal se requiere una consola de Administración.

3. Servicios de Protección contra Denegación (DDoS)

Para el "**Servicios de Protección contra Denegación (DDoS)**", **TOTALSEC, S.A. DE C.V.**, considera un servicio de protección basado enla nube que protege contra ataques de Denegación de Servicio Distribuido que se encuentran basados en firmas y volúmenes de conexión altos.

TOTALSEC, S.A. DE C.V., proporciona la continuidad del servicio conforme a lo siguiente:

- Continuidad y seguimiento del sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- **TOTALSEC, S.A. DE C.V.**, considera en su propuesta que la cantidad de tráfico máximo a inspeccionar por lo equipos y un ancho de banda de los enlaces de internet que estaran recibiendo los equipos, de al menos 1 Gbps en cada uno de los centros de datos.
- Garantiza el paso transaccional de datos legítimos, privilegiando la eliminación de tráfico anómalo dentro de los canales de comunicación del **Instituto.**
- Detección del tráfico basado en el lenguaje TCPDUMP (con información definida en las capas 3 y 4)
- Tiene la capacidad de advertir anticipadamente algún posible ataque, analizando tendencias de tráfico malicioso en tiempo real.
- Tiene la 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.
- Tiene la capacidad de monitoreo en tiempo real las subredes públicas que conectan los enlaces, para que permite la detección de tráfico anormal que pueda significar un ataque dirigida a ella.
- Detección de ataques basado en la línea de base contra los recursos definidos, con opciones configurables por recursos que permitan filtrar la sensibilidad de la anomalía y disparar un evento de tipo alerta, en paquetes por segundo y bytes por segundo.
- Soporta 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).
- Monitorea, de manera enunciativa más no limitativa, las siguientes variables en tiempo real:

- Para el protocolo IP:
  - ICMP
  - Paquetes IP fragmentados
  - Paquetes IP NULL
  - Paquetes IP con direcciones privadas
- Para el protocolo TCP:
  - Segmentos TCP NULL
  - Segmentos TCP RST
  - Segmentos SYN
  - Tráfico total

- Como mínimo detecta 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
- Permite la personalización de los niveles de alarma o umbrales que sirvan para la detección de ataques, a una granularidad por objeto monitoreado.
- Monitorea actividad sospechosa que pueda significar algún ataque de gusanos, virus, entre otros.
- Monitorea 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 incluyen fecha y hora de cada actividad realizada.
- Cuenta con la capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

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

TOTALSEC, S.A. DE C.V., proporciona la continuidad del servicio conforme a lo siguiente:
- Continuidad y seguimiento del sistema operativo propietario del fabricante, que recibe actualizaciones y parches de software conforme sean publicadas. Incluir un sistema operativo propietario del fabricante, que recibe actualizaciones y parches de software conforme sean publicadas.
- Incluye al menos 4 interfaces 10/100/1000 Gb, expandibles a interfaces 10Gb de ser necesario.
- Tiene un desempeño de al menos 2Gbps y 1,000,000 conexiones concurrentes
- Cuenta con la capacidad de permitir 50,000 nuevas conexiones por segundo.
- Incluye la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permite implementar reglas aplicadas a intervalos de tiempo específicos.
- Soporta alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Integra esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Permite la creación de grupos de usuarios.
- Permite delimitar la cantidad de conexiones por usuarios.
- Permite almacenar una base de usuarios local que permita realizar autenticación, sin depender de un servicio de autenticación externo.
- Cuenta con la capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
- Soporta DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKEv2.
- Soporta al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Soporta integridad de datos con md5, sha1 y sha2.
- Soporta las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Establece VPNs con gateways con direcciones IP dinámicas públicas.
- Crea una única asociación de seguridad (SA) por par de redes o subredes.
- Realiza VPNs SSL.
- Soporta la conexión desde dispositivos móviles y de escritorio a través de un cliente de acceso remoto. Dicho cliente soporta al menos las siguientes plataformas operativas: MAC OS X desde v10.4.10, iOS desde v4, Android desde v4.2, Windows desde v7.

5. Filtrado de Contenido Web

Para el **"Filtrado de Contenido Web", TOTALSEC, S.A. DE C.V.,** considera un servicio de filtrado de contenido Web mediante políticas de acceso que permite controlar y filtrar la utilización de servicios de acceso a Internet, en función de roles y perfiles.

TOTALSEC, S.A. DE C.V., proporciona la continuidad del servicio conforme a lo siguiente:

- Continuidad y seguimiento del sistema operativo propietario del fabricante, que recibe actualizaciones y parches de software conforme sean publicadas. Incluir un sistema operativo propietario del fabricante, que recibe actualizaciones y parches de software conforme sean publicadas.
- Soportarde forma mínima 120,000 usuarios de forma simultánea.
- Integra esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Permite operar en modo de proxy explicito y/o proxy transparente.
- Mecanismos de autenticación tales como: archivos locales de contraseña NTLM, LDAP, RADIUS, Active Directory y certificados.
- Control de autenticaciones simultáneas con una misma cuenta de usuario.
- Cifrado de datos (usuario/contraseña) en el proceso de autenticación.
- Controlar e inspeccionar al menos los protocolos: HTTP, HTTPS (SSL), FTP, CIFS, MAPI, DNS, P2P, SOCKS (v4/v5), IM (AOL, MSN, Yahoo Messengers), TCP-Tunnel, MMS, RTSP.
- Catalogar las páginas por Dominio (o subdominio), URL o IP.
- Bloqueo de las amenazas emergentes más comunes como: pop-ups, banners, spyware, adware, compartición de archivos punto a punto (P2P file sharing).
- Clasificación en tiempo real de sitios en internet (on-the-fly) que aún no han sido asignados a alguna categoría (servicio automático de validación en línea del sitio para determinar si es malicioso en caso de no tenerlo asignado en alguna categoría).
- Monitoreo y bloqueo de aplicaciones P2P tales como: BitTorrent, eDonkey, Gnutella, Fasttrack.
- Permite 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.
- Permite la clasificación de URL (dominio o subdominio) o IP en una sola categoría.
- Permite el uso de expresiones regulares.
- Permite 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).
- Permite 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.
- Proporciona capacidades de administración y reporteo centralizado incluyendo control de acceso discrecional, control de versiones, auditoria de usuario, sistema y utilerías de restauración de configuración.
- Proporciona soporte de administración multisesión (múltiples administradores utilizando el servicio de administración centralizado), a través de una interfaz gráfica vía Web cifrada (HTTPS).

- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que incluye fecha y hora de cada actividad realizada.

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

Para el "**Servicios de Filtrado de Contenido de Correo (Antispam)**", **TOTALSEC, S.A. DE C.V.**, considera un servicio de protección de correos spam, programas maliciosos y ataques dirigidos.

TOTALSEC, S.A. DE C.V., proporciona la continuidad del servicio conforme a lo siguiente:

- Incluye un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Cuenta con la capacidad de hasta 1.5M de correos por hora
- Cuenta con una capacidad de por lo menos 120,000 usuarios
- 12 TB por equipo, en HA por lo menos 24 TB.
- Integra esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Cuenta con la capacidad de revisar tanto el correo entrante como el saliente.
- Escaneo y analiza el asunto, encabezados y el cuerpo de los correos recibidos y enviados.
- Cuenta 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, puede detectar estas palabras en archivos adjuntos.
- Cuenta con la 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.
- Cuenta con mecanismos para clasificar los remitentes por su origen y tomar decisiones de flujo y volumen en consecuencia. Además, cuenta 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.
- Cuenta con la capacidad para ofrecer el análisis de archivos comprimidos en los formatos más populares, incluyendo aquellos con 7 capas de compresión.
- Cuenta con la capacidad de detectar el verdadero formato de un archivo y permitir aplicar políticas basadas en este rubro.
- Cuenta con la 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.
- Cuenta con un módulo de bloqueo de correo electrónico no deseado con base en la reputación de cuentas de correo, dominios y direcciones IP.
- Cuenta con la capacidad para soportar la revisión de firmas DKIM en los encabezados de correos entrantes.
- Cuenta con actualizaciones para sus patrones y motores de detección de spam (heurística), phising y código malicioso.
- Cuenta con 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.

- Es capaz de recibir tráfico con conexiones seguras (TLS) y poder hacer conexiones con otros servidores bajo el mismo protocolo.
- Cuenta 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).
- Cuenta con 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.
- Cuenta con la capacidad para integrar excepciones, tanto en hosts remitentes como en destinatarios, así como para cuentas de usuarios o dominios específicos.
- Permite la creación de cuarentenas o carpetas de auditoría de correo, la cuarentena puede ser almacenada por la solución como mínimo 30 días.
- Cuando se encuentre contenido malicioso en cuerpo del correo y archivos adjuntos, puede 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.
- Detecta correos masivos con virus y removerlos además de los archivos adjuntos, incluyendo la característica de archivos adjuntos Zero-byte.
- Proporciona la facilidad de enviar notificaciones a los usuarios (cuentas de correo electrónico) cuando algún evento sospechoso sea detectado.
- Cuenta con la capacidad de integrar agentes que realicen la función de escaneo y detección de spam en activos de infraestructura o servicios de correo electrónico bajo plataformas operativas Linux y/o Windows.
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que incluye fecha y hora de cada actividad realizada. Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

7. Firewall Especializado en Servicios Web (WAF)

Para el servicio de **"Firewall Especializado en Servicios Web", TOTALSEC, S.A. DE C.V.**, considera un servicio protección de aplicaciones web de los ataques cibernéticos.

Especificaciones Técnicas:

TOTALSEC, S.A. DE C.V., proporciona la continuidad del servicio conforme a lo siguiente:

- Incluye un sistema operativo propietario del fabricante, que recibe actualizaciones y parches de software conforme sean publicadas.
- Integra esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Realiza Inspección y análisis de perfiles de comportamiento normal de usuarios para detectar y mitigar el uso anormal de aplicativos Web.
- Soporta un throughput de 5 Gbps en capa 7.

- Soporta 100,000 Transacciones por Segundo (TPS).
- **TOTALSEC, S.A. DE C.V.,** 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
- Cuenta con el Servicio de reputación para identificar y bloquear ataques automatizados y/o usuarios maliciosos.
- Cuenta con Detección de ataques por clientes automatizados y robots.
- Cuenta con Detección de URL rewriting u ofuscación del URL.
- Manejo de errores y reescritura de errores para aplicativos Web.
- Cuenta con la capacidad para soportar inspección del protocolo XML.
- Cuenta con certificado por organismos de la industria como ICSA Labs o PCI.
- Brinda Actualización automática de firmas de prevención contra código malicioso.
- Proporciona Parcheo sobre aplicativos Web contra vulnerabilidades nuevas o conocidas (parcheo virtual).
- Brinda Protección contra ataques/vulnerabilidades conocidas (OWASP), de manera enunciativa más no limitativa:
    - SQL injection
    - Cross Site Scripting
    - Cross Site Request Forgery
    - Sensitive Data Exposure
    - Security Misconfiguration
    - Broken Authentication and Session Management
    - Otras nuevas identificadas por OWASP
- Soportar formatos de mensaje:
    - Web 2.0
    - HTML
    - XHML
    - HTML5
    - XML
    - JSON
    - AJAX
    - FLASH
    - JavaScript.
- Soporta Protocolos: TCP v4 y v6, HTTP, HTTPS, SSL/TLS.
- Soporta 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 incluye fecha y hora de cada actividad realizada.
- Cuenat con la capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Soporta 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).
- **TOTALSEC, S.A. DE C.V.**, considera en su propuesta al menos 200 sitios/portales a proteger.

8. Servicios de Gestión Unificada de Amenazas (UTM)

Para el **"Servicios de Gestión Unificada de Amenazas (UTM)"**, **TOTALSEC, S.A. DE C.V.**, considera una plataforma de nueva generación encargada de consolidar múltiples funciones de seguridad y redes mediante un appliance unificado que protege a los sitios remotos y simplifica la infraestructura del IMSS.

Especificaciones Técnicas:
TOTALSEC, S.A. DE C.V., proporciona la continuidad del servicio conforme a lo siguiente:

Generales
- Incluye un sistema operativo endurecido propietario del fabricante, que recibe actualizaciones y parches de software conforme sean publicadas.
- Soporta alta disponibilidad en modo Activo/Activo y Activo/Pasivo.

Funcionalidad Firewall
- Está 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.
- Incluye la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permite implementar reglas aplicadas a intervalos de tiempo específicos.
- Soporta y opera bajo protocolos de ruteo BGP y OSPF.
- Soporta y opera mediante rutas estáticas.
- Realiza inspección en capa 3 y 4.

Funcionalidad IPS

- Brinda soporte de al menos: 1,000,000 conexiones simultáneas por cada Gigabit de inspección.
- Latencia máxima de 0.5 milisegundos.
- Las Interfaces de Inspección operan 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 es capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado
- Cuenta con la capacidad de detección en línea sin bloquear tráfico (Modo transparente). El sistema sólo alertará que eventos serían bloqueados.
- Cuenta con la 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 contempla 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.
- Brinda reconocimiento de Tuneleo de Protocolos que permite la identificación de protocolos aun cuando estos estén encapsulados.
- Cuenta con detección de re-ensamblaje de paquetes fragmentados.
- Cuenta con integración de Listas Blanca (IP whitelist) mediante una lista de direcciones IP "confiables" que el sistema no bloqueará.
- Cuenta con la 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

- Permite operar en modo de proxy explícito y/o proxy transparente.
- Controla e inspecciona al menos los protocolos: HTTP, HTTPS (SSL).
- Cataloga las páginas por Dominio (o subdominio), URL o IP.
- Permite 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.
- Permite la creación de categorías de filtrado personalizadas, así como la creación de listas blancas y negras de filtrado URL.
- Cuenta con la capacidad de evitar la ejecución de códigos maliciosos.
- Permite 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

- Incluye la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permite almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Cuenta con la capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
- Soporta DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKE v2.
- Soporta al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Soporta integridad de datos con md5, sha1 y sha2.
- Soporta las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Establece VPNs con gateways con direcciones IP dinámicas públicas.
- Crea una única asociación de seguridad (SA) por par de redes o subredes.
- Soporta 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).

9. Firewall Especializado en Base de Datos

Para el servicio de **"Firewall Especializado en Servicios Web", TOTALSEC, S.A. DE C.V.**, considera un servicio protección de base de datos contra ataques cibernéticos.

Especificaciones Técnicas:

TOTALSEC, S.A. DE C.V., proporciona la continuidad del servicio conforme a lo siguiente:

- Tecnología de autoaprendizaje con mínima intervención humana, el proceso es constante y aprende estructura de bases de datos, incluyendo schemas, objetos, tablas; sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario.
- Opera a nivel local y en la capa de red
- Soporta al menos los siguientes motores de Bases de Datos:
  - Microsoft SQL Server
  - Oracle
  - Sybase
  - Informix
  - MySQL
  - Progress
  - PostgreSQL
- Proporciona 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, este soporta al menos los siguientes Sistemas Operativos:
  - AIX
  - HP-UX
  - Solaris
  - RHEL
  - SuSE
  - OEL

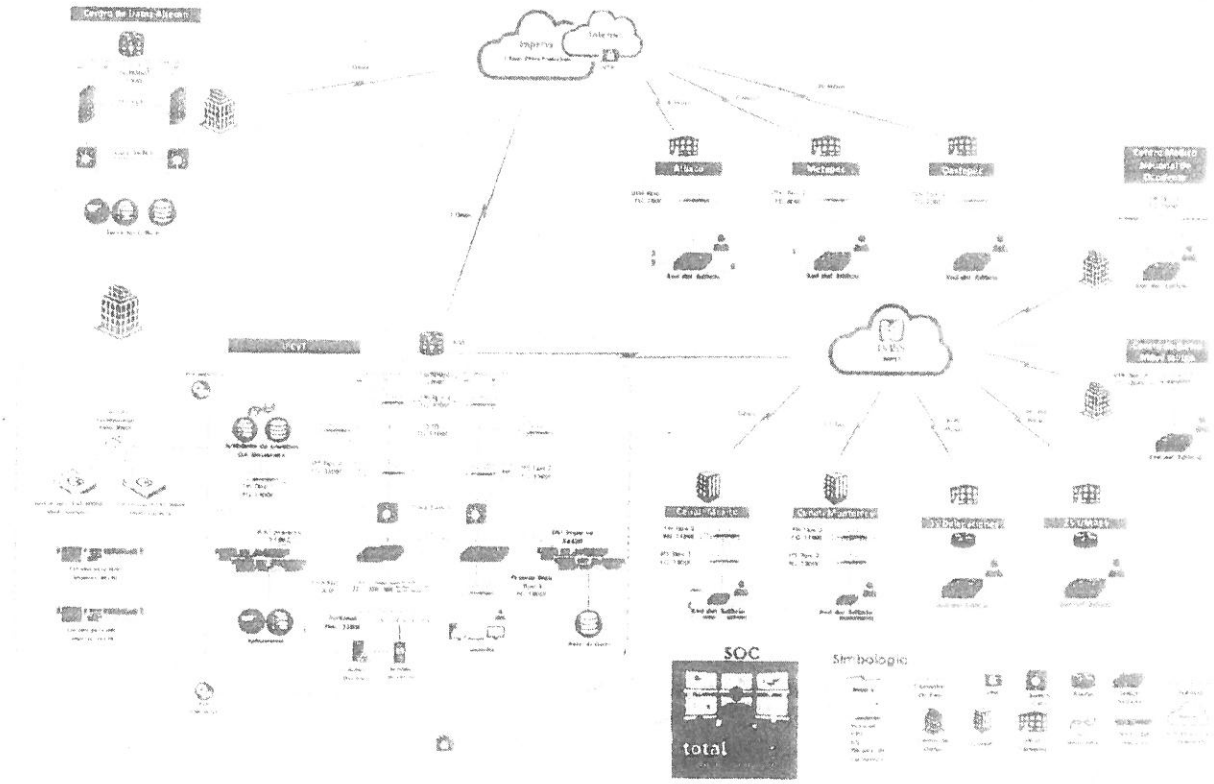
  - Windows 32/64 bits
- Cuenta con la capacidad para funcionar independiente a la activación de la auditoría nativa de la base de datos.
- Soporta el modo Transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
- Se requiere un repositorio para el registro de la actividad, es 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.
- Es 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.
- Cuenta con la 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.
- Cuenta con la capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo a las políticas de negocio. La definición de tipo de dato puede crearse de manera flexible y granular.
- Cuenta con la 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.
- Apoya en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y Control de cambios.
- Monitorea toda la actividad de las bases de datos, y almacena los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
- Monitorea e interactua 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.
- Hace 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.
- Cuenta con la capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.
- Cuenta con la capacidad para proveer detalles sobre alertas ya sean falsos positivos o negativos y tiene la facilidad de cambiar una política desde la alerta.
- Maneja reglas y políticas tan amplias o granulares como se requieran y puede ser construidas automática o manualmente y puede ser actualizadas, igualmente, de forma manual o automática.
- Las políticas granulares para control de acceso o generación de alertas cuentan con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios pueden usarse en cualquier número y cualquier combinación:
  - Número de registros a regresar por la consulta (SQL Query)
  - Número de registros afectados
  - Tipo de datos accesado (financiero, recursos humanos, inventarios, o cualquier definición personalizada)
  - Acceso a datos marcados como sensibles
  - Base de Datos, Schema, Instancia, Tabla y Columna accesada
  - Estado de autenticación de la sesión

  - Usuario y/o Grupo de Usuarios de Base de Datos conectado
  - Usuario conectado en la capa aplicativa, a diferencia del usuario conectado a la DB
  - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier customización por expresiones regulares)
  - Logins, Logouts, Queries
  - IPs de origen y destino
  - Nombre de Host origen, Usuario firmado en el Host origen
  - Aplicación usada para la conexión a la base de datos
  - Tiempo de respuesta/procesamiento del query
  - Errores en el manejador de SQL
  - Número de ocurrencias en intervalos de tiempo definidos
  - Por operaciones básicas (Select, Insert, Update, Delete)
  - Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export)
  - Por Stored Procedure o Function utilizada
  - Si existe ticket asignado de cambios
  - Hora del Día
- Posibilita los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.
- Protege contra ataques SQL y no-SQL.
- Cuenta 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.
- Considera de emergencia, para potenciales violaciones de la información que incluyen, 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.
- Maneja una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.
- Tiene 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)
- Tiene 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.
- Cuenta con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual presenta la documentación respectiva en el descubrimiento de las mismas.
- Soporta y aplica simultáneamente un modelo de seguridad positivo y negativo.
- El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que además cumplir con las siguientes especificaciones:
  - Bloquea las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
  - Incluye una lista pre-configurada y detallada de las firmas de ataque.
  - Emite la modificación o adición de firmas por el administrador.
  - Permite la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
  - Detecta ataques conocidos a nivel base de datos

- Cuenta con la capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Soporta 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).

Diagrama general de la Solución

A continuación, **Totalsec S.A de C.V** presenta el diagrama general de la solución con relación al servicio de "SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA CONTINUIDAD" (SASI-C) 2022



ATENTAMENTE

Víctor Rodríguez Fuentes
Apoderado Legal de Totalsec S.A de C.V.

totalsec
Expertos en Ciberseguridad

"TÉRMINOS Y CONDICIONES"

Investigación de Mercado para la contratación de los "Servicios Administrados de Seguridad Informática Continuidad (SASI-C)"

OBJETIVO DEL DOCUMENTO
Establecer las necesidades y condiciones de entrega los Servicios Administrados de Seguridad Informática Continuidad (SASI-C).

PREMISA
Las bases de datos, aplicaciones y cualquier otro tipo de información utilizado en el suministro de los servicios o a la que se tenga acceso derivado de la naturaleza de los mismos, que sean propiedad exclusiva del **Instituto** Mexicano del Seguro Social ("EL **INSTITUTO**") continuarán siendo propiedad exclusiva del mismo. En ese sentido, **TOTALSEC, S.A. DE C.V.**, se obliga a utilizarlas exclusivamente para cubrir los servicios requeridos.
TOTALSEC, S.A. DE C.V., presenta 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 a "EL **INSTITUTO**".

NOMBRE DEL PROYECTO
Investigación de Mercado para la contratación de los "Servicios Administrados de Seguridad Informática Continuidad (SASI-C)"

OBJETIVO 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 garanticen la continuidad operativa, de negocios y de seguridad de la información del **Instituto** que:
Garantice la continuidad operativa, la continuidad del negocio y la continuidad de la seguridad de la información de la Institución, durante la vigencia del presente contrato, especialmente durante la toma de operación y la transición de los servicios de los contratos anteriores (SASI) a los servicios propios de SASI-C.
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, y contención de ataques que puedan presentarse en la infraestructura de cómputo, sistemas y aplicaciones del **Instituto**.
Cuente con servicios de infraestructura regulados por niveles de servicio, que: implementen (instalen, migren habiliten y pongan a punto) los componentes necesario en los Centros de Datos del **Instituto** 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 servicios de seguridad de la información, que complementen el esquema de seguridad institucional de forma consistente y robusta, con el control, aseguramiento, diagnóstico, protección, pruebas, metodologías, de distintos rubros como el de acceso a cuentas privilegiadas, base de datos, aplicaciones, fuentes múltiples, vulnerabilidades, investigación forense y de procesos de seguridad, así como con otros servicios especializados en materia de seguridad y tecnologías de la información.

Contar con los Servicios Administrados de Seguridad Informática Continuidad para los activos de información donde se alojan los aplicativos, sistemas de información y bases de datos sensibles del

ANEXOS
DIVISIÓN DE CONTRATOS

Instituto, en las ubicaciones en donde los requiera el **Instituto**, así como con los niveles de servicio establecidos en el apéndice del presente documento y conforme a las características técnicas solicitadas en el Anexo Técnico.

SOLICITUD DE APEGO A NORMAS OFICIALES O CERTIFICACIONES
Se indica específicamente en el punto 13 del Anexo Técnico del presente proyecto.

VISITAS A INSTALACIONES
No se requiere.

TIPO DE ABASTECIMIENTO REQUERIDO
El **Instituto** requiere recibir los servicios objeto del Anexo Técnico con las funcionalidades descritas y en apego a los tiempos definidos.

GARANTÍAS
TOTALSEC, S.A. DE C.V., se obliga a constituir en la forma y términos previstos por los artículos 48 y 49 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 103 de su Reglamento y numerales 4.30 y 4.30.3 de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del **Instituto** Mexicano del Seguro Social, la garantía de cumplimiento divisible correspondiente.
En cualquier momento, "EL **INSTITUTO**" podrá hacer válida la Póliza de Garantía del contrato en caso de que **TOTALSEC, S.A. DE C.V.**, no cumpla con los tiempos y plazos de entrega establecidos en los presentes Términos y Condiciones.
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, **TOTALSEC, S.A. DE C.V.**, se compromete a entregar, dentro de los 10 (diez) días naturales a partir del día siguiente al de la notificación de la adjudicación del inicio de los servicios la garantía en los términos aquí señalados, 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.

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 **TOTALSEC, S.A. DE C.V.**, por escrito en papel membretado de su empresa, dicha solicitud se 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 a **TOTALSEC, S.A. DE C.V.**, 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.

Ejecución de la garantía

Se hará efectiva la garantía relativa al cumplimiento del contrato cuando:

TOTALSEC, S.A. DE C.V., incumpla con cualquiera de las obligaciones establecidas en el contrato que se celebre.

Se rescinda administrativamente el contrato.

La ejecución de la garantía será con independencia de la aplicación de las Penas Convencionales que procedan y de la rescisión administrativa del contrato.

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

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

ACUERDOS DE NIVEL 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 **TOTALSEC, S.A. DE C.V.**,

Procurar que los servicios de sean proporcionados con la calidad prevista.

Con fundamento en lo dispuesto por el Artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el **Instituto** aplicará penas convencionales por el atraso en la prestación del servicio basado en el importe del servicio prestado con atraso conforme al plan de trabajo y los plazos previstos, en el entendido de que esta penalización no excederá al importe de la garantía de cumplimiento de contrato.

Penas Convencionales

Se aplicarán penas convencionales por incumplimiento en el plazo de prestación de los servicios por parte de **TOTALSEC, S.A. DE C.V.**, del 0.2% por cada día natural de atraso en el inicio en la prestación del servicio, respecto del valor máximo total del contrato.

Servicios de Habilitación, Operación y Transición

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENSIONAL MENSUAL	CÓMPUTO DE LA PENALIZACIÓN
Plan de Trabajo detallado de los servicios del proyecto	15 días naturales posterior 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 OLA	15 días naturales posterior 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 posterior 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 de **TOTALSEC, S.A. DE C.V.**, , firmado por el representante legal,	15 días naturales posterior a la emisión del fallo	1% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

ANEXOS
DIVISIÓN DE CONTRATOS

donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios			

Servicios de Seguridad – Continuidad Operativa

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENSIONAL MENSUAL	CÓMPUTO DE LA PENALIZACIÓN
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 las 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

Servicios de Seguridad – **Verificación/Calidad**

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENSIONAL MENSUAL	CÓMPUTO DE LA PENALIZACIÓN
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
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

Procedimientos de Operación del servicio Servicio de Análisis de Vulnerabilidades, Servicios de Pruebas de Penetración Servicios de Análisis Forense Servicios de Borrado Seguro de Información Servicio de Gestión de Dominios Servicio de Certificados Digitales SSL	10 días hábiles 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
Metodología para la continuidad de los servicios Servicios de Sistema de Gestión de Seguridad de la Información (SGSI) Servicios de Gestión del Cambio en Seguridad de la Información	10 días hábiles 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

Servicios del Centro de Operaciones de Seguridad (SOC)

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENSIONAL MENSUAL	CÓMPUTO DE LA PENALIZACIÓN
Procesos de operación implementados: Requerimientos Cambios Configuraciones Incidentes Problemas Monitoreo	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

Matriz de Escalación Técnica y Organizacional	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
Procedimiento de operación de la Mesa de Servicios: Requerimientos Cambios Configuraciones Incidentes Problemas Monitoreo	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
Plan de Recuperación en caso de desastre (DRP)	60 días naturales posterior a la integración de las mesas de trabajo	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

Deducciones

Durante la vida 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 **TOTALSEC, S.A. DE C.V.**, 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 **TOTALSEC, S.A. DE C.V.**, se aplicarán deductivas conforme lo siguiente rubros:

Disponibilidad

La disponibilidad se define como la medida del porcentaje de tiempo, en que el sistema que brinda el servicio de seguridad de SASI-C (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 tiene que haber estado disponible.

Las mediciones de disponibilidad serán realizadas por **TOTALSEC, S.A. DE C.V.**, 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.

Se realizarán mediciones de disponibilidad desde el inicio del periodo operacional de los servicios de infraestructura SASI-C, para todos los módulos o posiciones de servicio contratados.

TOTALSEC, S.A. DE C.V., compromete la disponibilidad en base a los siguientes factores:

Incluye todos los componentes WAN, LAN, dispositivos de seguridad, y demás dispositivos que soportan al servicio de seguridad, así como su equivalente de configuración lógica.
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 de **TOTALSEC, S.A. DE C.V.**, estándosele aquellos períodos de indisponibilidad cuya responsabilidad no sea atribuible a **TOTALSEC, S.A. DE C.V.** 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 caídas de tráfico imputable a infraestructura de **TOTALSEC, S.A. DE C.V.**

Solo es calculada en base a fallas imputables a **TOTALSEC, S.A. DE C.V.**

Disponibilidad por sitio y por Posición de Servicio

Las caídas originadas por falla de energía responsabilidad del **Instituto** no serán tomadas en cuenta para la disponibilidad.

$$\text{Disponibilidad\_del\_Servicio} = \left\{ \frac{\text{Tiempo\_Total} - (\text{Tiempo\_Indisponible} - \text{Tiempo\_Instituto})}{\text{Tiempo\_Total}} \right\} \times 100$$

Donde:
Tiempo Total: Tiempo total de disponibilidad para el mes de medición.
Tiempo Indisponible: Tiempo indisponible según plataforma de monitoreo.
Tiempo **Instituto**: Tiempos atribuibles al **Instituto** extraídos del sistema de administración de incidentes.

Objetivos por métrica:

Disponibilidad Servicio	% Disponibilidad
Servicios de Seguridad – Continuidad Operativa	99.99%
Servicios de Seguridad – Verificación y Calidad	99.97%
Servicios del Centro de Operaciones de Seguridad (SOC)	99.99%

Deductiva por incumplimiento:

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Cuando no se cumplan con los objetivos de servicio, para los	% Disponibilidad conforme la tabla de objetivos	Minuto	0.5% por cada minuto de indisponibilidad	Valor unitario de la facturación mensual del servicio

diferentes niveles de disponibilidad, conforme al esquema de medición propuesto				relacionado con el incumplimiento

Tiempo de Detección y Solución de Fallas

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 serán realizadas por **TOTALSEC, S.A. DE C.V.**, usando su correspondiente herramienta de gestión y monitoreo del servicio. **TOTALSEC, S.A. DE C.V.**, realizará esta medición en un periodo mensual considerando el promedio del tiempo de solución para cada tipo de severidad. La metodología que se realice, las herramientas y los responsables sobre las mediciones, quedarán definidos en las mesas de trabajo.

El Tiempo de Solución a Fallas se divide en tres casos, en función de la severidad, causa e impacto de los mismos:

Severidad 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.

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 serán atendidos por ingenieros de **TOTALSEC, S.A. DE C.V.**, 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 **TOTALSEC, S.A. DE C.V.**, 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 posterior a la detección de la falla	2 horas posterior al registro y notificación de la falla
Alta	Representa una falla en la que hay una degradación que impide la operación de un servicio, mismo que soporta una función de negocio del **Instituto** pero que no tiene un impacto a nivel nacional.	20 minutos posterior a la detección de la falla	4 horas posterior al registro y notificación de la falla
Media	Representa una falla menor que impide la operación de un servicio, mismo que afecta a un grupo de usuarios reducido del **Instituto.**	120 minutos posterior a la detección de la falla	48 horas posterior al registro y notificación de la falla
Baja	Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad, tienen un bajo impacto en la operación del negocio y su atención y/o solución puede ser calendarizada.	5 días hábiles posterior a la detección de la falla	Se define entre el **Instituto** y **TOTALSEC, S.A. DE C.V.**, conforme las mesas de trabajo que se establezcan para este propósito.

Deductiva por incumplimiento:

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Tiempo máximo de registro y notificación conforme al nivel de severidad critica	10 minutos posterior al registro y notificación de la falla	Minuto	0.1% 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	2 horas posterior al registro y	Hora	0.5% por cada hora o fracción de atraso en la	Valor unitario de la facturación mensual del

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
de severidad critica	notificación de la falla		solución de la falla	servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad alta	20 minutos posterior al registro y notificación de la falla	Minuto	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad alta	4 horas posterior 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 posterior al registro y notificación de la falla	Minuto	0.1% 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 posterior 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 posterior al registro y notificación de la falla	Día	0.1% 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 **TOTALSEC, S.A. DE C.V.**, conforme las mesas de trabajo que se establezcan para este propósito.	Día	0.5% por cada día de atraso en la solución de la falla conforme la fecha establecida en las mesas de trabajo	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Tiempo de Detección y Mitigación de Incidentes

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 estandarizaao; es la evidencia inequívoca de que la confidencialidad, integridad y disponibilidad de la información ha sido vulnerada.

Las métricas de tiempo para la actividad sospechosa se refieren al tiempo de notificación y envió de dictamen que **TOTALSEC, S.A. DE C.V.**, realizará ante el **Instituto** al momento de detectar una actividad sospechosa. Ante una actividad sospechosa, **TOTALSEC, S.A. DE C.V.**, registrará y notificará al personal del **Instituto** en máximo 30 minutos. Posterior a su detección y registro, se emitirá un dictamen de actividad sospechosa con recomendaciones para erradicarla, este dictamen será enviado al personal del **Instituto** en máximo 90 minutos.

Las métricas para el tiempo de registro y notificación se refieren al tiempo en que **TOTALSEC, S.A. DE C.V.**, avisa al **Instituto** cuando ha confirmado un incidente de seguridad, ésta métrica se realizará en los tiempos definidos según la prioridad a partir de que se apertura algún registro relacionado con un incidente de seguridad. La métrica de tiempo de contención se refiere a que, tras la detección del incidente, **TOTALSEC, S.A. DE C.V.**, detendrá y aislará el mismo según los tiempos definidos para cada prioridad.

Las mediciones serán realizadas por **TOTALSEC, S.A. DE C.V.**, de SASI-C usando su correspondiente herramienta de gestión y monitoreo del servicio. **TOTALSEC, S.A. DE C.V.**, realizará esta medición en un periodo mensual según el nivel de servicio para cada tipo de métrica y/o prioridad.

Objetivos de la métrica:

SEVERIDAD	AFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
Critica	Representa un incidente de alto impacto que impide la operación total de un servicio, mismo que soporta una función de negocio del **Instituto** a nivel nacional.	10 minutos posterior a la detección del incidente	60 minutos posterior al registro y notificación del incidente
Alta	Representa un incidente en el que hay una degradación que impide la operación de un servicio, mismo que soporta una función de negocio del **Instituto** pero que no	20 minutos posterior a la detección del incidente	240 minutos posterior al registro y notificación del incidente

SEVERIDAD	AFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
	tiene un impacto a nivel nacional.		
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 posterior 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 posterior al registro y notificación del incidente

Deductiva por incumplimiento:

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Registro y notificación de Actividad Sospechosa	30 minutos posterior 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 posterior 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	LIMITE DE INCUMPLIMIENTO
Tiempo máximo de registro y notificación conforme al nivel de severidad critica	10 minutos posterior al registro y notificación del incidente	Minuto	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad critica	60 minutos posterior 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 alta	20 minutos posterior 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 alta	240 minutos posterior 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 posterior 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 posterior 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 bajo	60 minutos posterior 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

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Tiempo máximo de solución conforme al nivel de severidad baja	2,880 minutos posterior 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

Solicitudes de Requerimientos y Cambios

Es el tiempo que tarda **TOTALSEC, S.A. DE C.V.**, en realizar un alta, cambio o baja sobre la infraestructura del servicio en seguridad, basada en el menú de configuraciones comunes preestablecidas durante las mesas de trabajo correspondientes. Estas configuraciones serán acorde a las necesidades de conectividad y flujos de información de las aplicaciones del **Instituto**, entendiendo que la complicación para su atención es menor dado que se tiene la experiencia y el conocimiento de las mismas configuraciones de los módulos de los servicios de seguridad en operación.

Objetivos de la métrica:

Requerimientos

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 posterior a la solicitud formal por parte del **Instituto**	60 minutos posterior al registro realizado por el **Instituto**
Media	Requerimiento generado por parte del **Instituto** a fin de atender a necesidades de operación comunes.	30 minutos posterior a la solicitud formal por parte del **Instituto**	480 minutos posterior al registro realizado por el **Instituto**
Baja	Requerimiento generado por parte del **Instituto** a fin de atender a necesidades de operación programadas.	60 minutos posterior a la solicitud formal por parte del **Instituto**	1,440 minutos posterior al registro realizado por el **Instituto**

Cambios

PRIORIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE EJECUCIÓN
Emergente	Cambios requeridos como resultado de una pérdida repentina del servicio, fallo en un activo de infraestructura o a petición del **Instituto**.	1 hora posterior a la solicitud formal por parte del **Instituto**	Conforme al plan de trabajo definido entre el **Instituto** y **TOTALSEC, S.A. DE C.V.,**
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 serán analizados y aprobados por el **Instituto**.	1 hora posterior a la solicitud formal por parte del **Instituto**	Conforme al plan de trabajo definido entre el **Instituto** y **TOTALSEC, S.A. DE C.V.,**
Estándar	Cambios en los servicio 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 posterior a la solicitud formal por parte del **Instituto**	24 horas posterior al registro realizado por el **Instituto**

Cualquier cambio ejecutado por **TOTALSEC, S.A. DE C.V.,** , mismo que no se encuentre autorizado por el **Instituto**, derive o no en alguna falla de los servicios de seguridad, será catalogado como un incidente de seguridad, mismo que será clasificado con base en las afectaciones o riesgos que pudieron generar.

Deductiva por incumplimiento:

Requerimientos

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Tiempo máximo de registro y	10 minutos posterior al	Minuto	0.1% por cada minuto de atraso	Valor unitario de la facturación

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
notificación conforme al nivel de prioridad Alta	registro y notificación del requerimiento		en el registro y notificación	mensual del servicio relacionado con el incumplimiento
Tiempo máximo de ejecución conforme al nivel de prioridad Alta	60 minutos posterior 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 posterior al registro y notificación del requerimiento	Minuto	0.1% 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 posterior 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 posterior al registro y notificación del requerimiento	Minuto	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Baja	24 horas posterior 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	LIMITE DE INCUMPLIMIENTO
Tiempo máximo de registro y notificación conforme al nivel de prioridad Emergente	60 minutos posterior al registro y notificación del cambio	Minuto	0.1% 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 **TOTALSEC, S.A. DE C.V.,**	Hora	5% 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 posterior al registro y notificación del cambio	Minuto	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Normal	Conforme al plan de trabajo definido entre el **Instituto** y **TOTALSEC, S.A. DE C.V.,**	Hora	5% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Estándar	60 minutos posterior al registro y notificación del cambio	Minuto	0.1% 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 posterior al registro y notificación del cambio	Hora	5% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Servicios de Seguridad – Continuidad Operativa

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Reportes Técnicos de los activos de infraestructura que contemplen: Disponibilidad Controles de Cambios Requerimientos Incidentes/Fallas Actividad Sospechosa Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	5 días hábiles posterior 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

Servicios de Seguridad – Verificación/Calidad

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Reportes Técnicos de los activos de infraestructura que contemplen: Disponibilidad Controles de Cambios Requerimientos Incidentes/Fallas Actividad Sospechosa Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	5 días hábiles posterior al cumplimiento del mes vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Servicios de Análisis de Vulnerabilidades: 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 posterior a la solicitud generada por parte del **Instituto**	Día	2% 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 Prueba de Penetración: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las	10 días hábiles posterior a la solicitud generada por parte del **Instituto**	Día	2% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
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				
Servicios de Análisis Forense: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de infraestructura verificados	15 días hábiles posterior a la solicitud generada por parte del **Instituto**	Día	2% 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 Borrado Seguro de Información:	5 días hábiles posterior a la solicitud generada por	Día	2% por cada día hábil de atraso en la entrega de los	Valor unitario de la facturación mensual del servicio

ANEXOS
DIVISIÓN DE CONTRATOS

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
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.	parte del **Instituto**		reportes técnicos/ejecutivos	relacionado con el incumplimiento
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.	5 días hábiles posterior a la solicitud generada por parte del **Instituto**	Día	2% 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 Certificados Digitales SSL: Reporte Técnico y Ejecutivo en	1 día hábil posterior a la solicitud generada por parte del **Instituto**	Día	2% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
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)				el incumplimiento
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 posterior a la solicitud generada por parte del **Instituto**	Día	2% por cada día hábil de atraso en la entrega del plan de trabajo	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Sistema de Gestión de Seguridad de la Información: Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora del Sistemas De Gestión de Seguridad de la Información (SGSI)	Conforme a la fecha estipulada en el plan de trabajo acordado entre el **Instituto** y **TOTALSEC, S.A. DE C.V.,**	Día	2% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, por evento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Servicios de Red – Continuidad Operativa

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Reportes Técnicos de los activos de infraestructura que contemplen: Disponibilidad Controles de Cambios Requerimientos Incidentes/Fallas Actividad Sospechosa Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	5 días hábiles posterior 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

Servicios del Centro de Operaciones de Seguridad (SOC)

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	5 días hábiles posterior 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 posterior al cumplimiento del mes vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados	5 días hábiles posterior 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 posterior 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 posterior 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 posterior 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 posterior 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

ANEXOS
DIVISIÓN DE CONTRATOS

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Creación de cuentas de acceso en las consolas de administración de los servicios de seguridad	5 días hábiles posterior 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 posterior 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 posterior 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 posterior a la ejecución de la ventana mantenimiento	Día	2% 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	5 días hábiles posterior a la solicitud generada por parte del **Instituto**	Día	2% por cada día hábil de atraso en la entrega del reporte	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	LIMITE DE INCUMPLIMIENTO
soluciones de seguridad				
Reporte Técnico de las configuraciones de las soluciones de seguridad	5 días hábiles posterior a la solicitud generada por parte del **Instituto**	Día	2% 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 posterior a la solicitud generada por parte del **Instituto**	Día	2% 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 posterior a la solicitud generada por parte del **Instituto**	Día	2% 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 posterior a la solicitud generada por parte del **Instituto**	Día	2% 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 posterior a la solicitud generada por parte del **Instituto**	Día	2% 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	Día	2% por cada día hábil de atraso en la entrega de los reportes de	Valor unitario de la facturación mensual del servicio

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
	los Centro de Datos o donde lo indique el **Instituto**, conforme cada solución integrada y posterior a la integración de las mesas de trabajo		actividades, por periodo, por evento	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

CONDICIONES DE PAGO

E administrador de contrato será el servidor público responsable de administrar y supervisar el cumplimiento de las obligaciones pactadas en el mismo.

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, será el responsable de recibir y aceptar cada uno de "Los Servicios", así como realizará los trámites de pago en cumplimiento al procedimiento administrativos vigente en "**EL INSTITUTO**".

Para proceder a la liberación de pago, el Titular 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 contractuales a cargo de **TOTALSEC, S.A. DE C.V.,** , así como de la ejecución, validación, técnica y administrativa de todos y cada uno de los documentos que acreditan que los servicios proporcionados por **TOTALSEC, S.A. DE C.V.,** se cumplieron en tiempo, forma y cantidad y que cumplen con las características, especificaciones y condiciones requeridas, procederá el pago de conformidad con lo establecido en el artículo 51 de la LAASSP.

La forma de pago a **TOTALSEC, S.A. DE C.V.,** será la estipulada en el contrato 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.

TOTALSEC, S.A. DE C.V., entregará en la División de Trámite de Erogaciones, situada en la calle de 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 **TOTALSEC, S.A. DE C.V.,** , 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 **TOTALSEC, S.A. DE C.V.**, 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, a mes vencido conforme a las entregas programadas.

ENTREGABLES

TOTALSEC, S.A. DE C.V., entregará al Titular de la División de Seguridad Informática Física dependiente de la Coordinación de Telecomunicaciones y Seguridad de la Información:

Entregables Generales

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto	Única Vez	15 días naturales posterior a la emisión del fallo
	Documento Compromiso de suscripción de OLAs	Única Vez	15 días naturales posterior a la emisión del fallo
	Matriz de Escalación	Única Vez	15 días naturales posterior a la emisión del fallo
	Escrito por parte de **TOTALSEC, S.A. DE C.V.**, , firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	Única Vez	15 días naturales posterior a la emisión del fallo
Servicios de Seguridad – Continuidad Operativa	Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a	Única Vez	5 días hábiles posteriores a la integración de las mesas de trabajo

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	implementar en los centros de datos o donde lo indique el **Instituto**		por cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el **Instituto**	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el **Instituto**, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad	Única Vez	20 días hábiles previo al termino 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	Única Vez	10 días hábiles posteriores a la integración de las

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Seguridad a implementar en los centros de datos o donde lo indique el **Instituto**		mesas de trabajo por cada servicio que se pretenda habilitar
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integran activos de infraestructura para su habilitación	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el **Instituto**, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad, que requieran integran activos de infraestructura para su habilitación	Única Vez	20 días hábiles previo al termino del contrato para aquellos servicios que se encuentren habilitados
Servicios de Análisis de Vulnerabilidades	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Pruebas de Penetración	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Análisis Forense	Procedimientos de Operación del servicios	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Borrado Seguro de Información	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicio de Gestión de Dominios	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)	Metodología de implementación de los servicios	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios del Centro de Operaciones de Seguridad (SOC)	Procesos de operación implementados: Requerimientos Cambios Configuraciones Incidentes Problemas Monitoreo	Única Vez	15 días naturales posterior a la emisión del fallo
	Matriz de Escalación Técnica y Organizacional	Única Vez	15 días naturales posterior a la emisión del fallo
	Procedimiento de operación de la Mesa de Servicios: Requerimientos Cambios Configuraciones Incidentes Problemas Monitoreo	Única Vez	15 días naturales posterior a la emisión del fallo
	Plan de Recuperación en caso de desastre (DRP)	Única Vez	60 días naturales posterior a la integración de las mesas de trabajo
	Expedientes Curriculares del personal del SOC	Única Vez	15 días naturales posterior 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 y red	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

Entregables Verificación Calidad

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades	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 posterior 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,	Evento	10 días hábiles posterior a la solicitud generada por parte del **Instituto**

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	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 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 posterior a la solicitud generada por parte del **Instituto**
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	Evento	5 días hábiles posterior a la solicitud generada por parte del **Instituto**

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	almacenamiento borrado.		
Servicio de Gestión de Dominios	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos.	Evento	5 días hábiles posterior 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 posterior a la solicitud generada por parte del **Instituto**
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	Evento	10 días hábiles posterior 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 posterior 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 posterior al término de la implementación de cualquier solución de seguridad o conforme cada solicitud generada por el **Instituto**

ANEXOS
DIVISIÓN DE CONTRATOS

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Actualización de la matriz de escalación	Evento	5 días hábiles posterior a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad
	Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad	Evento	5 días hábiles posterior a la ejecución de la ventana mantenimiento
	Reporte con Estadísticas de uso y desempeño (información analítica) de la soluciones de seguridad	Evento	5 días hábiles posterior a la solicitud generada por parte del **Instituto**
	Reporte Técnico de las configuraciones de las soluciones de seguridad	Evento	5 días hábiles posterior a la solicitud generada por parte del **Instituto**
	Reporte Técnico de los incidentes presentados en las soluciones de seguridad	Evento	5 días hábiles posterior a la solicitud generada por parte del **Instituto**
	Reporte Técnico de los requerimientos registrados en la mesa de servicios	Evento	5 días hábiles posterior a la solicitud generada por parte del **Instituto**
	Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y su diagroma de interrelación conforme fueron	Evento	5 días hábiles posterior a la solicitud generada por parte del **Instituto**

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	registrados en la CMDB		
	Diagramas de Arquitectura de las soluciones de seguridad	Evento	2 días hábiles posterior a la solicitud generada por parte del **Instituto**

Entregables Periódicos

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Seguridad – Continuidad Operativa	Reportes Técnicos de los activos de infraestructura que contemplen: 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 posterior al cumplimiento del mes vencido
Servicios de Seguridad – Verificación/Calidad	Reportes Técnicos de los activos de infraestructura que contemplen: 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 posterior al cumplimiento del mes vencido
	Reporte Técnico de los requerimientos	Mensual	5 días hábiles posterior al

Servicios del Centro de Operaciones de Seguridad (SOC)	generados a través de la Mesa de Servicios para los servicios de seguridad implementados		cumplimiento del mes vencido
	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posterior 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 posterior al cumplimiento del mes vencido
	Reporte de las evaluaciones operativas a los servicios de seguridad implementados	Trimestral	5 días hábiles posterior al cumplimiento de cada trimestre calendario
	Reporte que integre el calendario de actualizaciones de	Trimestral	5 días hábiles posterior al cumplimiento de

	versionamiento en software de cada servicio implementados		cada trimestre calendario

TOTALSEC, S.A. DE C.V., cumplirá con los formatos provistos por el **Instituto** y en apego al Normatividad Vigente.

CONDICIONES DE ACEPTACIÓN
Se formalizarán los entregables descritos en el numeral anterior a efecto de dar por recibido los servicios requeridos.
Todos los documentos serán entregados en papel membretado de la empresa de manera impresa y en electrónico.
Se entregará a la División de Seguridad Informática Física perteneciente a la Coordinación de Telecomunicaciones y Seguridad de la Información.

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.

CONVENIO DE CONFIDENCIALIDAD Y RESGUARDO DE LA INFORMACIÓN
TOTALSEC, S.A. DE C.V., se suscribirá el Convenio de Confidencialidad y Resguardo de Información correspondiente, en el que su representada o cualquiera de su personal asignado al proyecto por ningún motivo extraerán o divulgará el contenido de la información que se les entregará como parte del contrato.

Dicho documento estará firmado por su representante legal, en la que manifieste, que se compromete a respetar y seguir los estándares tecnológicos, tanto de metodologías, procedimientos, hardware, como de software definidos por el **Instituto.**

Asimismo, en dicha carta **TOTALSEC, S.A. DE C.V.**, indicará que se compromete a que toda la información que exista a la fecha de la adjudicación y aquella que desarrolle derivado del presente proyecto será propiedad intelectual y exclusiva de "EL **INSTITUTO**" y no podrá ser utilizada por **TOTALSEC, S.A. DE C.V.**, para otros fines.

Por lo que considera al menos los siguientes mecanismos de control de acceso a la información del **Instituto**:

ANEXOS
DIVISIÓN DE CONTRATOS

Se establece controles de acceso y privilegios restringidos al personal de **TOTALSEC, S.A. DE C.V.**, a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del **Instituto**.

Se implanta y acepta en todo momento el uso de controles que permitan registrar "Pistas de Auditoria" para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.

La seguridad lógica estará protegida mediante el uso de dispositivos de control de acceso (firewall's), mecanismos de encriptación y seguridad física entre las redes de **TOTALSEC, S.A. DE C.V.**, y las del **Instituto**.

El almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por **TOTALSEC, S.A. DE C.V.**, observando los requisitos de seguridad y resguardo de la información.

TOTALSEC, S.A. DE C.V., permitirá el acceso a información relacionada con el servicio prestado al **Instituto** para la realización de auditorías.

TOTALSEC, S.A. DE C.V., no hará uso indebido de la documentación, información, ni activos de TIC a los que tengan acceso o que se generen con motivo de la prestación del servicio.

PROPIEDAD INTELECTUAL

TOTALSEC, S.A. DE C.V., se obliga durante la garantía de las licencias a liberar a "EL **INSTITUTO**" de toda responsabilidad de carácter civil, mercantil, penal o administrativa que, en su caso, se ocasione con motivo de la infracción de derechos de autor, patentes, marcas u otros derechos de propiedad industrial o intelectual a nivel Nacional o Internacional.

MÉTODO DE EVALUACIÓN DE PROPUESTAS

Se evaluará mediante el criterio binario conforme a las características que presenten los proveedores en cuanto a funcionalidades en el Anexo Técnico como en el apéndice A del Anexo Técnico, con la finalidad de determinar la solvencia de las proposiciones a partir de verificar el cumplimento de las condiciones legales, técnicas y económicas.

FUNCIONARIOS PÚBLICOS DE LA DIDT PARTICIPANTES EN EL PROCESO DE ADQUISICIÓN

C. Fernando González Velázquez, Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información.
C. Abraham Gutiérrez Castillo, Titular de la División de Seguridad Informática Física.
C. Javier Melgoza Esqueda, Titular de la División de Seguridad Informática Lógica.
C. Cynthia Osmara Verdín Villegas, Jefe Área Nivel Central E0.

VIGENCIA DEL CONTRATO

La vigencia del contrato será a partir de la firma y hasta el **31 de agosto de 2022.**

PLAZO DEL SERVICIO

La prestación de los servicios iniciará a partir del día hábil siguiente al de la notificación de la adjudicación y hasta el 31 de agosto de 2022.

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:

Administrador del Contrato y Responsable Técnico; Titular de la División de Seguridad Informática Física y Titular de la División de Seguridad Informática Lógica
Supervisor del Contrato; Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información.
Los servicios a cargo de **TOTALSEC, S.A. DE C.V.**, estarán bajo la administración y supervisión del responsable designado que para tal efecto.

MECANISMOS DE CONTROL PARA LA ADMINISTRACIÓN DEL CONTRATO

El Administrador del Contrato en conjunto con **TOTALSEC, S.A. DE C.V.**, generarán el acta de entrega-recepción conforme a los entregables del Anexo Técnico.

MECANISMOS REQUERIDOS AL PROVEEDOR PARA RESPONDER POR DEFECTOS O VICIOS OCULTOS DE LOS BIENES O DE LA CALIDAD DE LOS SERVICIOS

No aplica

OTORGAMIENTO DE ANTICIPO

No aplica

ANEXOS
DIVISIÓN DE CONTRATOS

ANEXOS GENERALES

Investigación de Mercado para la contratación de los "Servicios Administrados de Seguridad Informática Continuidad (SASI-C)"

Esquema Estructural y Metodologías

ESQUEMA ESTRUCTURAL

ESQUEMA ESTRUCTURAL DE LA ORGANIZACIÓN DE LOS RECURSOS HUMANOS DEL PROYECTO

1 OBJETIVO

TOTALSEC, S.A. DE C.V., presenta la información referente a los contactos responsables involucrados enla provisión y gestión de los servicios del **IMSS**, a fin de garantizar el flujo de información y continuidaden los servicios y a su vez proporcionar los estándares por medio de los cuales se llevará a cabo elmanejo de información, cambios, fallas, alertas y notificaciones derivadas del servicio

2 ALCANCE

La información del documento aplica para todos aquellos contactos que se encuentren involucrados dentro de la solución provista por **TOTALSEC, S.A. DE C.V.**, en los servicios del **IMSS**.

3 LINEAMIENTOS

El personal designado como responsable por **TOTALSEC, S.A. DE C.V,** se encargará de llevar a cabo las actividades de implementación, puesta a punto, configuración, operación, cambios y notificaciones.

El flujo de información solo deberá efectuarse entre la mesa de servicio de SOC y el personal previamente definido en las matrices y tabla de operación, en caso de requerir la interacción con alguna área no establecida dentro de la matriz, deberá efectuar las notificaciones a través la mesa de servicio de SOC, propuesto por **TOTALSEC, S.A. DE C.V.**

Los horarios para la interacción y atención por parte del **IMSS** se realizarán bajo un esquema lunes a domingo de las 24 hrs, a través del único punto de contacto propuesto por **TOTALSEC, S.A. DE C.V.**, que será la mesa de servicio de SOC.

4 MECANISMO DE ATENCIÓN Y SEGUIMIENTO

A continuación, **TOTALSEC, S.A. DE C.V.**, detalla los siguientes medios de comunicación, podrá emplear los siguientes medios de comunicación para llevar a cabo la notificación e interacción con el personal designado por el IMSS.

- Email: soc@totalsec.com.mx
- Números: 17207777 opc 2 y 1
  (+52) 55 3010 3227

5 ESTRATEGIA OPERATIVA

La orientación de la propuesta, de **TOTALSEC, S.A. DE C.V.**, se define en un enfoque basado en procesos, lo que permite el buen manejo y desarrollo de la solución propuesta en el siguiente documento.

Este enfoque permite la mejora de los flujos de aceptación, atención y comunicación dentro de la operación, llevando a cambio el aseguramiento del servicio, acorde a los SLA definidos previamente por el **IMSS**.

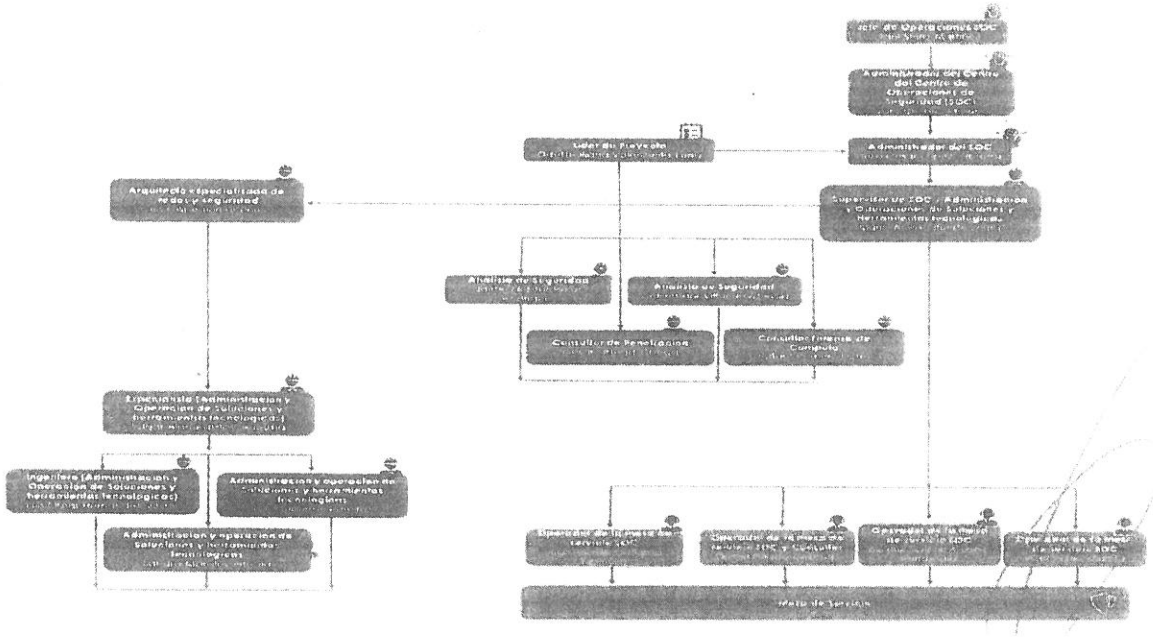
Esta estrategia se encuentra apegada al marco de referencia ISO 27001 e ISO20000, que rigen **TOTALSEC, S.A. DE C.V.**, con el cual cubrimos todos los aspectos relevantes de nuestra relación con el **IMSS**, permitiendo además tener un control completo de todas las interacciones que se generan de dicha relación.

El IMSS podrá por referirse **al apartado "Anexos Generales" al final de este documento en la sección llamada "Metodologías"**, para identificar los procedimientos, y los flujos operativos, parte de **TOTALSEC S.A. de C.V.**

6 ORGANIZACIÓN DE LOS RECURSOS HUMANOS

TOTALSEC, S.A. DE C.V., presenta el listado del personal que llevará a cabo las tareas necesarias para la prestación del **"SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA CONTINUIDAD (SASI-C)"** solicitados por **EL IMSS**, la cual se muestra en la siguiente imagen:

"SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA CONTINUIDAD" (SASI-C) 2022



En este Esquema estructural se integran recursos humanos relacionados a nuestro diseño de entrega de servicios (personal ampliado al descrito en **"Anexo Perfiles -totalsec"**

Dicho personal descrito en el documento en **"Anexo Perfiles -totalsec"** se encuentra completamente apegado a la matriz de puntos y porcentajes y los recursos ampliados en el presente son con la finalidad de mostrar el Esquema estructural en su totalidad para el servicio de la investigación de mercado del **SASI-C** sin impacto a los solicitados como mínimo. Es decir, se observan los requeridos y listados en cuanto a Roles a cubrir con recursos asignados al proyecto al ser propuesta de la estructura de nuestro diseño de entrega estructural y metodología de servicios descrita en **punto 6 Organización de los Recursos Humanos.**

7. ORGANIZACIÓN DE LOS RECURSOS HUMANOS

A continuación, **TOTALSEC, S.A. DE C.V.**, detalla la matriz de roles y funciones de las actividades que realizaran cada área mencionada en el esquema estructural comenzando por los perfiles o roles requeridos por la convocante y posteriormente el personal ampliado:

ROL [Función nominal]	**RESPONSABILIDADES / FUNCIONES ESPECÍFICAS** [Actividades que serán desempeñadas y de las cuales será responsable]
ADMINISTRADOR DEL CENTRO DE OPERACIONES DE SEGURIDAD	Responsable de la administración, monitoreo, operación de los servicios proporcionados por el SOC, así como del soporte, atención a fallas e incidentes de seguridad; En caso de evento o incidente, contar con la disponibilidad en 7 X 24 para cumplir el modelo de escalamiento a través del SOC **Nota: Para validar el cumplimiento de los "Perfiles" referirse al "Anexo Perfiles -totalsec"**
ADMINISTRACIÓN Y OPERACIÓN DE SOLUCIONES Y HERRAMIENTAS TECNOLÓGICAS	Personal que reúne amplios conocimientos técnicos y conoce las necesidades únicas del proyecto, experto en las soluciones propuestas y sus funciones son: **Actividades:** • Evita los problemas antes de que sucedan con una planificación proactiva, visitas y revisiones técnicas programadas de forma regular. • Responde a las solicitudes del cliente a nivel técnico en tiempo y forma y lo mantiene al corriente de los avances de las mismas. • Colabora mano a mano con el Project Manager. • En caso de evento o incidente, contar con la disponibilidad en 7 X 24 para cumplir el modelo de escalamiento a través del SOC **Nota: Para validar el cumplimiento de los "Perfiles" referirse al "Anexo Perfiles -totalsec"**

ANALISTA DE SEGURIDAD	Encargado de ejecutar las revisiones de seguridad sobre las aplicaciones y la infraestructura, así como prever, detectar, analizar, contener, erradicar, documentar incidente de seguridad; En caso de evento o incidente, contar con la disponibilidad en 7 X 24 para cumplir el modelo de escalamiento a través del SOC **Nota: Para validar el cumplimiento de los "Perfiles" referirse al "Anexo Perfiles -totalsec"**
LÍDER DE PROYECTO	Es la persona encargada de administrar y coordinar el proyecto. El personal asignado es capaz de proponer los lineamientos, estándares y metodología del proyecto. **Actividades:** • Delega adecuadamente tareas del proyecto para cumplir el mismo en tiempoy forma. • Realiza reuniones con el equipo de trabajo para detectar y prevenir a tiempoposibles desvíos y tomar medidas correctivas. • Detecta necesidades de capacitación del equipo del proyecto para lograr una formación adecuada, alineada al desarrollo profesional de los colaboradores. • Reduce significativamente los riesgos, mediante la adhesión a políticas comunicacionales abiertas, permitiendo que cada uno de los participantes enel proyecto tenga la oportunidad de expresar sus opiniones y preocupaciones. • Controla los costos, tiempos y calidad en el proyecto. • Tiene conciencia de los recursos con los que se cuenta para el buen términodel proyecto. **Nota: Para validar el cumplimiento de los "Perfiles" referirse a Anexo Perfiles -totalsec.**
OPERADOR DE LA MESA DE SERVICIO SOC	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. **Actividades:** • Soporte. • Atención a fallas e incidentes que se presenten en la interoperabilidad con otros proveedores y/o fabricantes. • Atención de consultas respecto de la gestión, adiciones, cambios, configuración, optimización u obtención de información de los equipos que forman parte del presente proyecto.

	Nota: Para validar el cumplimiento de los "Perfiles" referirse a Anexo Perfiles -totalsec.
CONSULTOR DE PENETRACIÓN	Personal encargado de 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. En caso de evento o incidente, contar con la disponibilidad en 7 X 24 para cumplir el modelo de escalamiento a través del SOC **Nota: Para validar el cumplimiento de los "Perfiles" referirse a Anexo Perfiles -totalsec.**
CONSULTOR FORENSE DE CÓMPUTO	Personal encargado de 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. En caso de evento o incidente, contar con la disponibilidad en 7 X 24 para cumplir el modelo de escalamiento a través del SOC **Nota: Para validar el cumplimiento de los "Perfiles" referirse a Anexo Perfiles -totalsec.**
ARQUITECTO ESPECIALIZADO EN REDES Y SEGURIDAD	Responsable de la administración,monitoreo, operación de los servicios proporcionados por el SOC, en lo que a servicios de interconexión de red se refiere. **Actividades:** • Soporte. • Atención a fallas e incidentes que se presenten en la interoperabilidad con otros proveedores y/o fabricantes. **Nota: Para validar el cumplimiento de los "Perfiles" referirse a Anexo Perfiles -totalsec.**

METODOLOGÍAS

1. DESCRIPCIÓN DE METODOLOGÍA SOC

1.1. Objetivo

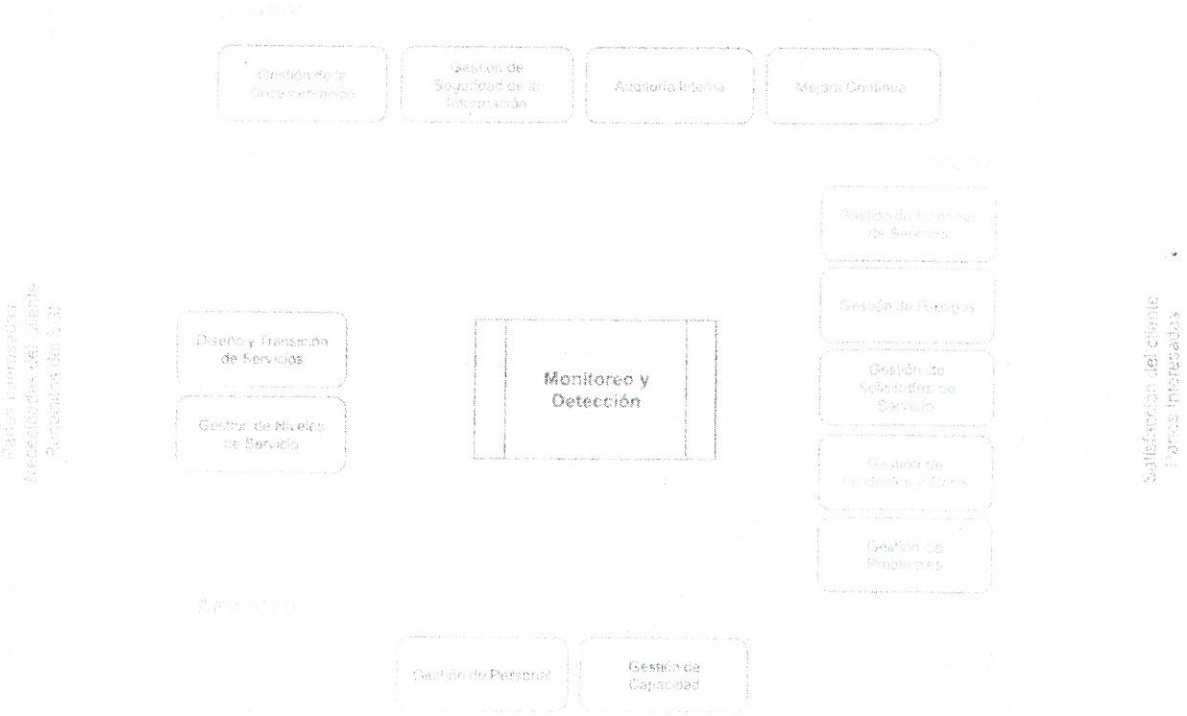
Monitorear todos los sucesos que se presenten, identificando aquellos que deben ser analizados para determinar si tienen algun impacto negativo que pudiera afectar la operación de los servicios que brinda el SOC y que puedan derivar en un incidente o solicitud de servicio.

1.2. Alcance

Todos aquellos servicios que estén integrados en la arquitectura de seguridad del cliente y que este en monitoreo serán responsabilidad de **TOTALSEC, S.A. DE C.V.**, de la misma forma **TOTALSEC, S.A. DE C.V.**, podrá recomendar redefinir o rediseñar la arquitectura de seguridad para optimizar recursos en beneficio del cliente.

El personal de **TOTALSEC, S.A. DE C.V.**, asignado a las operaciones del SOC revisará activamente la información proveniente de los eventos de las soluciones administradas y notificar al **IMSS** los reportes de hallazgos. Asimismo, participará en diversas actividades de seguridad de la información incluyendo: Monitoreo de Incidentes de Seguridad, reporte de incidentes potenciales y escalamiento; todos los incidentes serán registrados y se dará seguimiento con los niveles de criticidad acordes a cada evento. El SOC continuamente construirá y ajustará las reglas para la detección posibles incidentes en las soluciones propuestas, actualizándose de acuerdo a las tendencias de ataques de las amenazas informáticas.

1.2.1. Diagrama de Flujo de SOC



Cuando se presente una situación de falla o incidente, se abrirá un ticket en la herramienta de administración de incidentes y se debe dar inicio al proceso de solución, incluye soporte de primer, segundo y tercer nivel, de la siguiente manera:

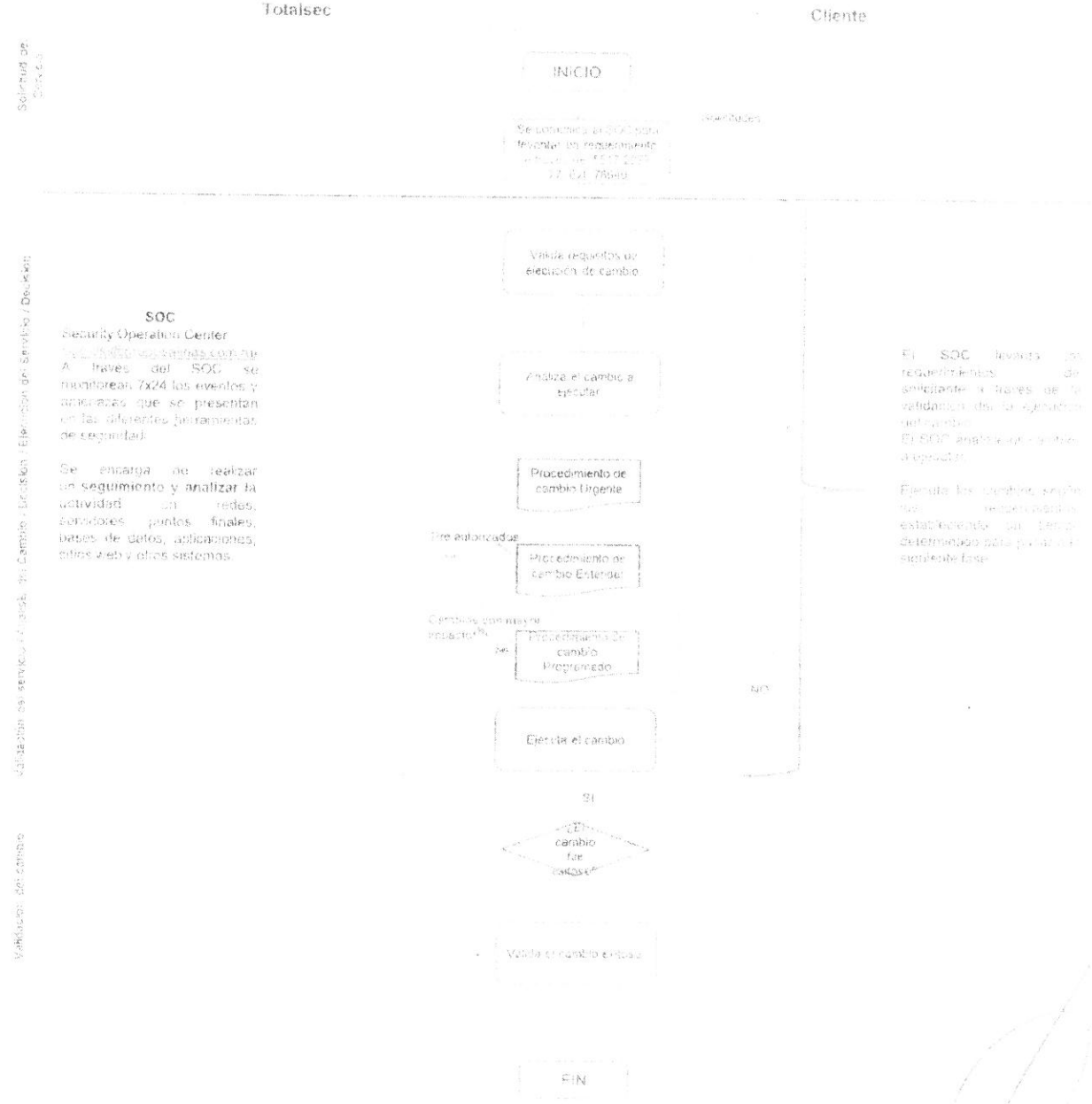
- Soporte de primer nivel: Se proporcionará remotamente a través del SOC. (24X7x365)
- Soporte de segundo nivel: Cuando la falla debe ser escalado hacia los ingenieros de segundo para atender de forma remota.
- Soporte de tercer nivel: El centro de operaciones escalará el problema al fabricante del equipo en cuestión y dará seguimiento hasta su solución.

A continuación, se indican los medios de comunicación

- **Email: soc@totalsec.com.mx**
- **Números: 17207777 opc 2 y 1**
  (+52) 55 3010 3227

TOTALSEC S.A de C.V desarrollará una plataforma en ambiente web pública, donde se reportarán fallas, problemas, incidentes, métricas, de manera que el IMSS pueda tener acceso para toma de decisiones, está definición se realizará en mesas de trabajo para revisar el alcance junto con el IMSS, una vez se presente el fallo.

1.2.2 Flujo de Operación del SOC



A continuación, **TOTALSEC, S.A. DE C.V.**, describe los procesos con los que desarrollará las actividades del servicio del centro de operaciones de seguridad (SOC) para cumplimiento de la partida III del presente investigación de mercado del **SASI-C**, en caso de contingencia y de continuidad operativa.

Se cuentan procesos operativos para almenos los siguientes rubros, del servicio del centro de operaciones de seguridad (SOC) indicado en la convocante del **IMSS**:

- Administración de Dispositivos.
- Administración de Requerimientos.
- Administración de Cambios.
- Administración de Configuraciones.
- Administración de Vulnerabilidades.
- Administración de Incidentes.
- Administración de Problemas.
- Investigación de Incidentes.

1.2.3 Descripción de Actividades para Altas, Bajas y Cambios de SOC

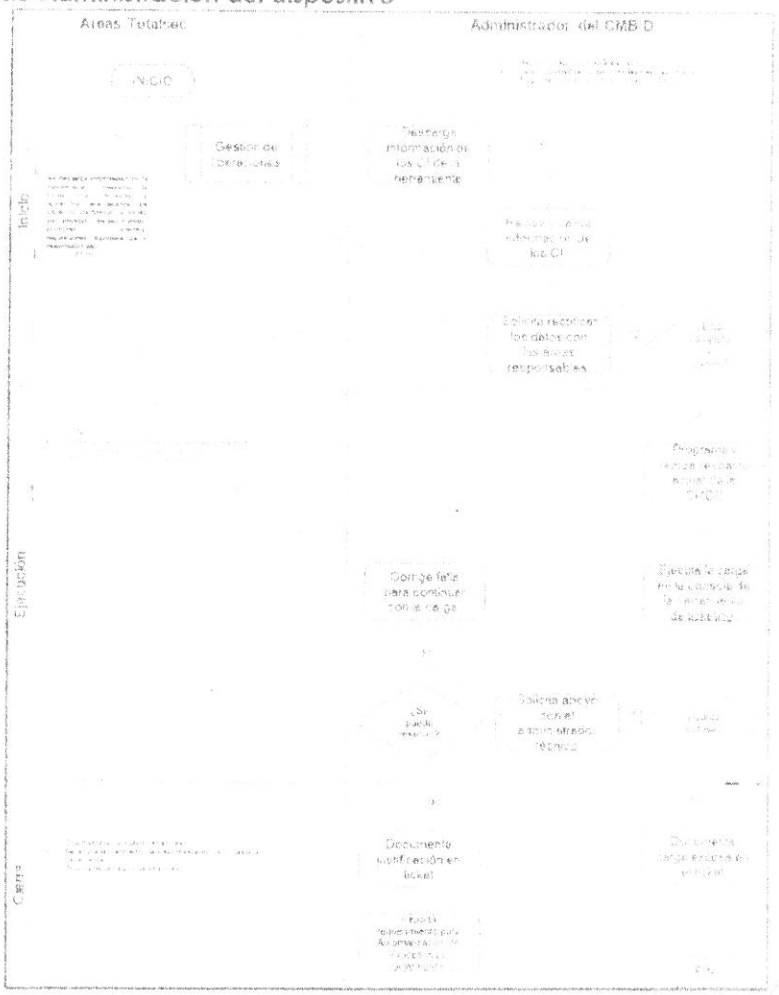
Fase	Actividad	Responsable
Solicitud del servicio	El cliente se comunica con el SOC para levantar un requerimiento por medio del teléfono 5517207777 ext. 76640	Solicitante
Validación del servicio	El SOC levanta los requerimientos del solicitate y valida la ejecución del cambio	SOC
Análisis del cambio	El SOC analiza los cambios a ejecutar.	SOC
Decisión	¿Qué tipo de cambio se requiere? Procedimiento de cambio urgente Procedimiento de cambio estándar Procedimiento de cambio programado	SOC
Ejecución del servicio	Ejecuta los cambios según los requerimientos estableciendo un tiempo de estabilización	SOC
Decisión	¿El cambio fue exitoso? Si, pasar a la fase de análisis del cambio No, pasar a la siguiente fase	SOC
Validación del cambio	Valida el cambio exitoso de los requerimientos solicitados.	Solicitante

1.3 Administración del dispositivo y configuraciones

TOTALSEC, S.A. DE C.V., garantiza que la Administración de Dispositivos y la Base de Datos de Gestión de Configuración (CMDB, "Configuration Management Data Base"), se mantenga actualizada con información precisa y fiable con los CI requeridos para proporcionar un servicio, incluyendo sus relaciones; mediante la gestión y revisión periódica de la misma.

Todos los CIs relacionados con los servicios que suministra **TOTALSEC, S.A. DE C.V.**, a través del SOC ("Security Operation Center") y de forma indirecta, los CIs que el **IMSS** entrega al SOC para su gestión

1.3.1 Flujo de Administración del dispositivo



1.3.2 Descripción de actividades para ABC de dispositivos

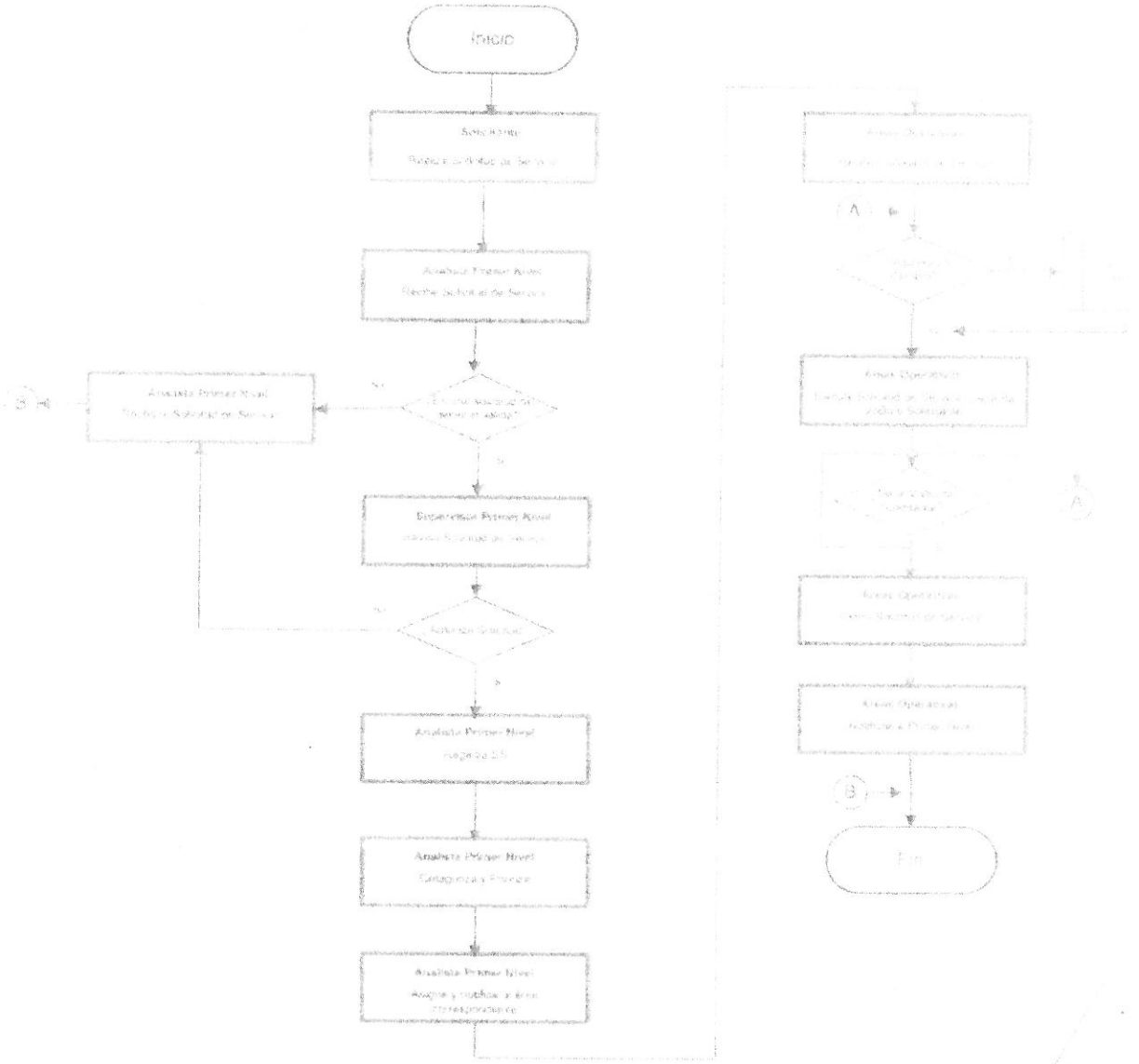
Fase	Actividad	Responsable
Validación	1. Se descarga información de la herramienta	SOC
	2. Revisa y valida información de los CI	
Decisión	¿Está completa y vigente?	SOC
	Si pasar a la fase 4	
	No, pasar a la fase 3	
	3. Solicita rectificar los datos con las áreas responsables	
Espera	Pasar a la fase 2	SOC
	4. Programa y realiza respaldo actual del CDMB	
	5. Ejecuta la carga en la consola de la herramienta ticketing	
Decisión	¿Carga exitosa?	SOC
	Si, pasar a la fase 10	
	No, pasar a la fase 6	
Ejecución	6. Solicita apoyo con el administrador técnico	SOC
Decisión	¿Se puede resolver?	SOC
	Si, pasar a la fase 7	
	No, pasar a la fase 8	
Ejecución	7. Corrige la falla para continuar con la carga	SOC
	Seguir con la fase 5	
	8. Documenta la justificación en ticket	
Cierre	9. Reporta requerimiento para automatización de procesos en Governance	SOC
	10. Documenta carga exitosa en el ticket	

1.3.3 Administración de requerimientos

TOTALSEC, S.A. DE C.V., proporciona atención a todas las solicitudes de servicio recibidas y que se encuentren en el alcance de la investigación de mercado del **(SASI-C)** emitida por el **IMSS**, con la finalidad de facilitar información y acceso rápido a los servicios estándar por medio del SOC ofrecidos por **TOTALSEC, S.A. DE C.V.**

ANEXOS
DIVISIÓN DE CONTRATOS

1.3.4 Flujo de Administración de requerimientos



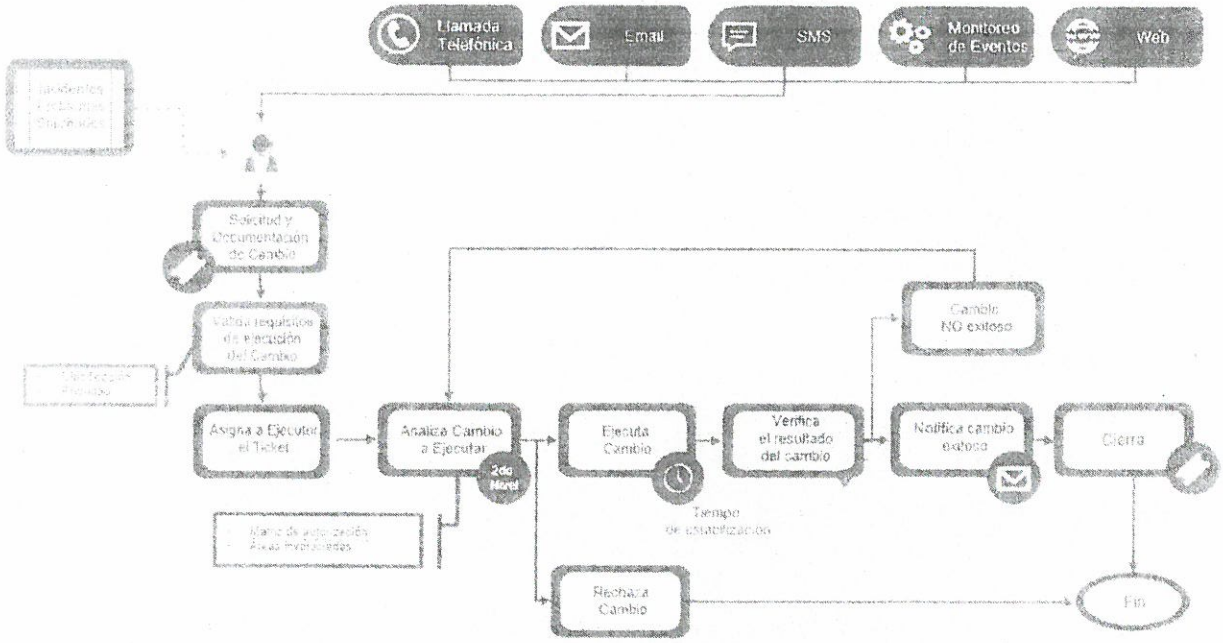
1.4 Administración de cambios

TOTALSEC, S.A. DE C.V., establece las actividades que garantizan que todo cambio en los servicios proporcionados ante el IMSS sea planificado, evaluado, aprobado, implementado y documentado.

1.4.1 Alcance

Revisar que se realicen e implementen adecuadamente todos los cambios en TI.

1.4.2 Flujo de Administración de administración de cambios

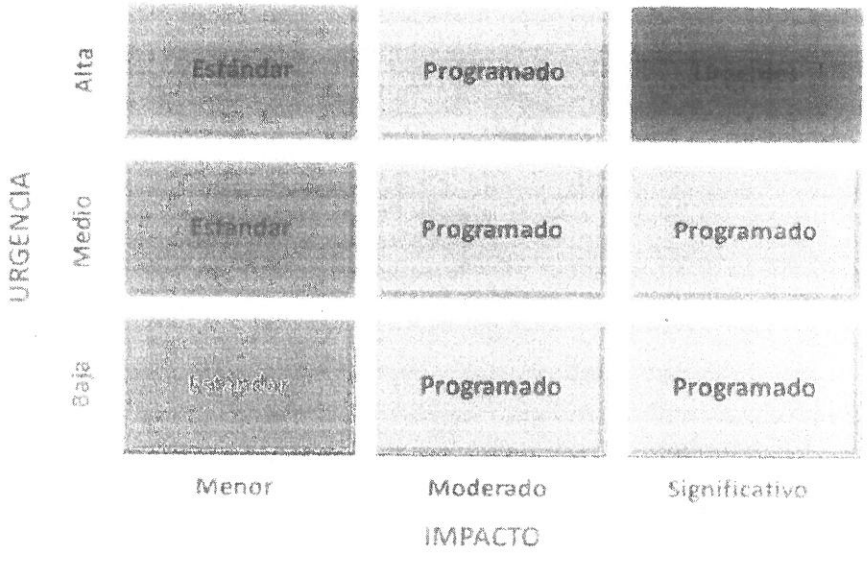


1.4.3 Descripción del ABC de actividades para cambios

Fase	Actividad	Responsable
Solicitud del cambio	El divide se comunica con el SOC para levantar un requerimiento por medio de [illegible] ext. 7866)	Solicitante
Aprobación del cambio	El SOC revisa los requerimientos de [illegible] valida la ejecución del cambio	SOC
Clasificación	El SOC clasifica el cambio [illegible] ¿Qué tipo de cambio se requiere? Procedimiento de cambio urgente Procedimiento de cambio estándar Procedimiento de cambio programado	SOC
Ejecución del servicio	Ejecuta los cambios según los requerimientos establecidos en tiempo de ejecución	SOC
Cierre	¿El cambio fue exitoso? Si pasa a la fase de análisis del cambio No pasa a la siguiente fase	SOC
Validación del servicio	Valida el cambio exitoso de los requerimientos solicitados	SOC

1.4.4 Priorización

TOTALSEC, S.A. DE C.V., presenta el modelo para priorizar los cambios los controles de cambio se utiliza la siguiente referencia:



1.5 Administración de vulnerabilidades y pruebas de penetración

TOTALSEC, S.A. DE C.V., normar el Análisis de Vulnerabilidades efectuado por el área de Certificación de Seguridad

1.5.1 Alcance

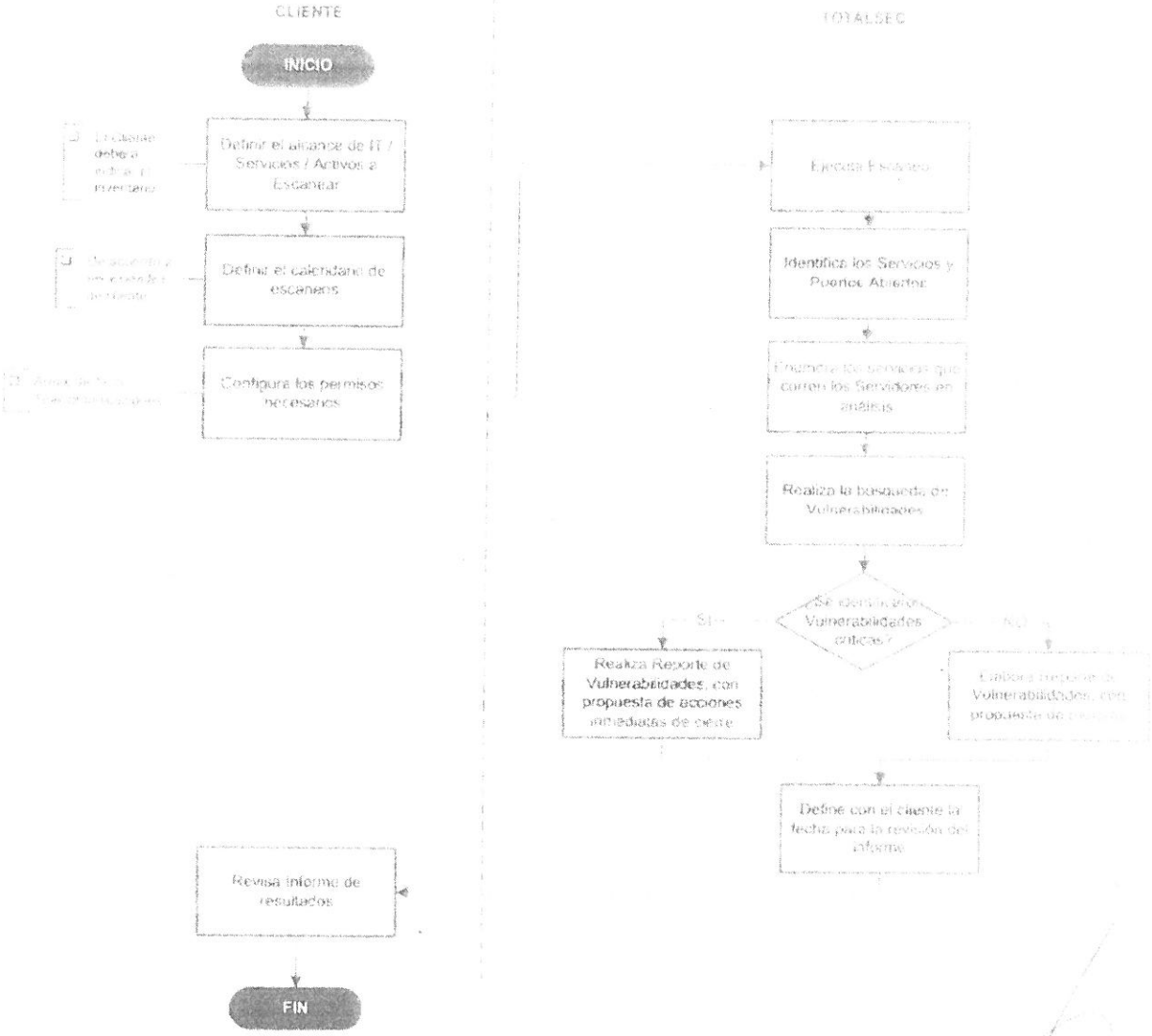
El alcance de este documento considera desde la ejecución del escaneo, la identificación y clasificación de las vulnerabilidades, su análisis y propuestas de remediación.

Revisar activamente la información proveniente de los eventos de las soluciones administradas y notificar los reportes de hallazgos. Asimismo, participamos en diversas actividades de seguridad de la información incluyendo: Monitoreo de incidentes de seguridad, reporte de incidentes potenciales y escalamiento; todos los incidentes los dejamos registrados y damos seguimiento con los niveles de criticidad acordes a cada evento.

Una vez realizada el análisis de vulnerabilidades, **TOTALSEC, S.A. DE C.V.**, estará pendiente junto con el personal del IMSS de aplicar las actualizaciones y parches de seguridad de forma continua para la infraestructura de seguridad que forma parte de este servicio; esta actividad se realizará bajo un plan de trabajo.

ANEXOS
DIVISIÓN DE CONTRATOS

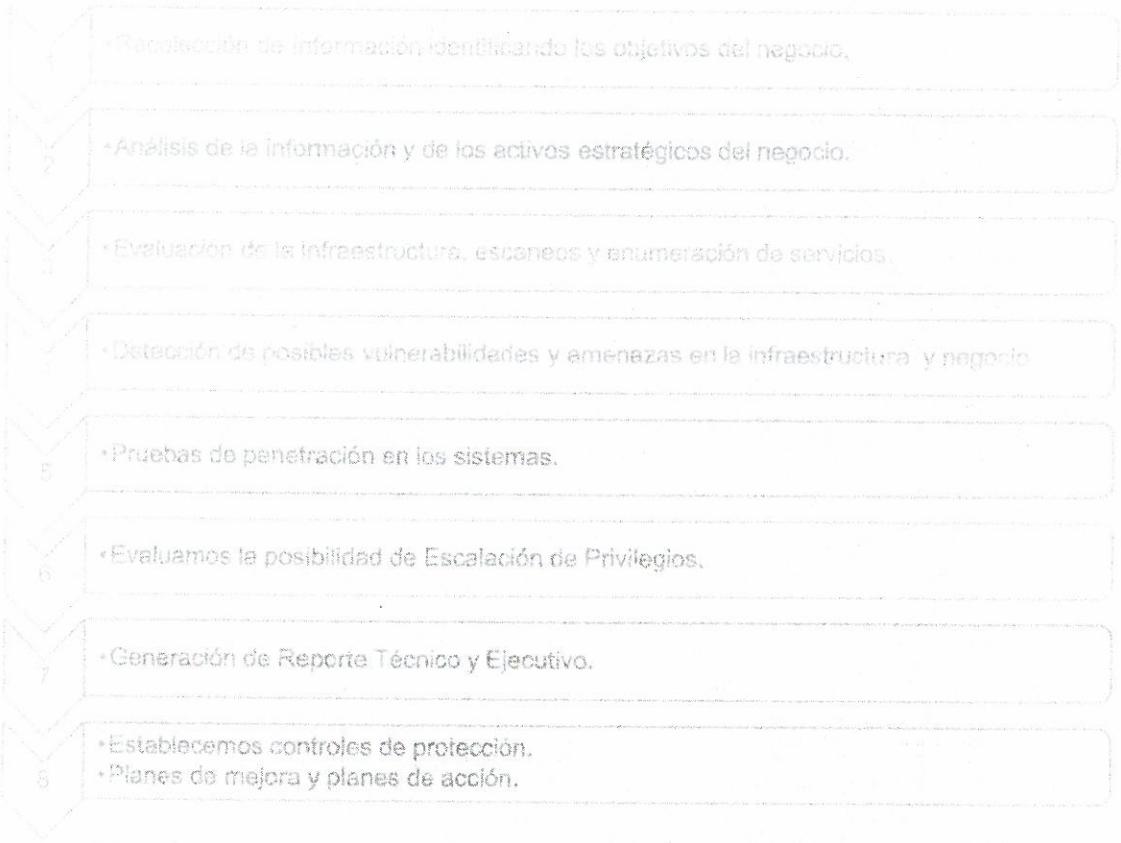
1.5.2 Flujo de Administración de análisis de vulnerabilidades y pruebas de penetración



Para este cumplimiento, **TOTALSEC, S.A. DE C.V.**, utilizará y proporcionará la descripción de la metodología del Proyecto Abierto de Seguridad en Aplicaciones Web (Open Web Application Security Project, OWASP).

Descripción de la metodología de Proyecto Abierto de Seguridad en Aplicaciones Web (Open Web Application Security Project, OWASP).

TOTALSEC, S.A. DE C.V., cuenta con la capacidad de integrar en su proposición su metodología de Análisis de Vulnerabilidades y Pruebas de Penetración, OWASP



(a) Imagen la metodología OWASP

A continuación, **TOTALSEC, S.A. DE C.V.** describe el detalle de cada fase de la metodología sobre OWASP para dar cumplimiento a los entregables.

La principal metodología utilizada por **TOTALSEC, S.A. DE C.V.** para las pruebas de análisis de vulnerabilidades y pruebas de penetración de aplicaciones Web se basa en los estándares de Web Application Test Metodología de Open Web Application Security Project (OWASP).

Provee las bases teóricas para realizar pruebas de intrusión sobre aplicaciones web. Se llevan a cabo todas las pruebas descritas en el manual de OWASP Test Guide 4.0.

ANEXOS
DIVISIÓN DE CONTRATOS

- **Recolección de Información identificando los objetivos del negocio, en este caso IMSS**

  - **TOTALSEC, S.A. DE C.V.**, en común acuerdo con **IMSS**, debe definir el alcance de los objetivos a explotar de acuerdo a los riesgos que **IMSS** ve como potencialmente vulnerables, dichos objetivos sera clasificados por prioridades como es. AAA+, AAA, y AA.

  - La clasificación de los activos como **TOTALSEC, S.A. DE C.V.**, significan lo siguiente:
    - AAA+ Dispositivos, aplicaciones o servicios críticos, los cuales su afectación podría paralizar totalmente la continuidad operativa de IMSS.

    - AAA Dispositivos, aplicaciones o servicios importantes, los cuales su afectación limita la operatividad de servicios relevantes, como podría ser la liberación de pagos, conciliación de datos personales, empresariales o financieros.

    - AA Dispositivos, aplicaciones o servicios relevantes pero que su afectación limita de manera parcial ó alguna vertical de la institución, que, si bien genera riesgos, hay continuidad, hay operación y que uno de los daños mayores que puede presentar es la imagen del área tecnológica, operativa ó de IMSS.

- **Análisis de la información y de los activos estratégicos del negocio, en este caso IMSS.**

  - Una vez que el IMSS declare los activos que TOTALSEC, S.A. DE C.V. realizara los análisis correspondientes, TOTALSEC, S.A. DE C.V. programará la actividad de acuerdo a un plan de trabajo, enumerara los objetivos a explotar y solicitara el visto bueno del IMSS para comenzar con las pruebas correspondientes.

- **Evaluación de la infraestructura, escaneos y enumeración de servicios, en este caso IMSS.**

  - **TOTALSEC, S.A. DE C.V.**, con herramientas licenciadas y de propiedad de **TOTALSEC, S.A. DE C.V.**, llevará a cabo los escaneos de reconocimiento que dará como primer resultado la visión de alcance y la posición en donde se encuentra el personal asignando para atacar por parte de TOTALSEC, S.A. DE C.V.

  - De igual forma en esta primera revisión los hallazgos que no requieren ataques dirigidos y que pueden ser clasificados como los primeros a tratar de vulnerar y en su momento comprometer.

- **Detección de posibles vulnerabilidades y amenazas en la infraestructura y negocio, en este caso IMSS.**

  - De acuerdo a las pruebas de vulnerabilidad que ejecute **TOTALSEC, S.A. DE C.V.**, permitirá clasificar aquellas que son de mayor riesgo para el IMSS, mismas que con

autorización y acuerdo con el IMSS, TOTALSEC, S.A. DE C.V. buscara comprometer en una ventana de tiempo que autorice el IMSS.

- **Pruebas de penetración en los sistemas.**

  - En esta fase, TOTALSEC, S.A. DE C.V. abra ejecutado las pruebas correspondientes con herramientas licenciadas de propósito (propiedad de TOTALSEC, S.A. DE C.V.), donde explotará los hallazgos a fin de identificar el impacto, el nivel de riesgo y exposición con el que se encuentra el objetivo.

- **Evaluamos la posibilidad de Escalación de Privilegios.**

  - Una vez comprometido el objetivo, TOTALSEC, S.A. DE C.V. buscará escalar los privilegios a medida de obtener el control se podrá determinar si el objetivo comprometido puede afectar ó dañar la imagen pública, ó si en su defecto puede alcanzar otros objetivos considerados críticos ó importante, ó en su defecto el contenido de los mismos, como datos personales, datos financieros ó datos clasificados como confidenciales.

- **Generación de Reporte Técnico y Ejecutivo.**

  - TOTALSEC, S.A. DE C.V. preparará un reporte detallado de los hallazgos y sus vulnerabilidades, la trazabilidad del compromiso, la enumeración con su detalle de los activos comprometidos a fin de que el IMSS pueda revisar, cotejar y posteriormente eliminar los hallazgos, así como las recomendaciones a seguir a fin de mitigar la causa raíz del riesgo.

  - Todo reporte se prepara con análisis técnico, se expondrá los riesgos operativos ó impactos negativos que afectara de manera directa a TOTALSEC, S.A. DE C.V., dicho reporte se presentará ilustrado donde se señale puntualmente la vulnerabilidad que concluya en un riesgo para la institución.

  - **TOTALSEC, S.A. DE C.V.,** entregará un reporte ejecutivo a los tomadores de decisión que facilite al personal de **IMSS** corregir los hallazgos de manera inmediata, así como sentar la base de una solución definitiva, que conlleve a un monitoreo, validar o implementar el control de cambios, así como un plan para aplicar actualizaciones de parches, firmware o reemplazo de infraestructuras.

- **Establecemos controles de protección.**

  - **TOTALSEC, S.A. DE C.V.,** propondrá soluciones de control, dichos controles puede ser reforzando sobre servicios de seguridad que actualmente cuente el IMSS, ajustar los niveles de visibilidad con los que cuenta el **IMSS**, aplicar controles documentales que permita al IMSS a dejar registro de posibles cambios y en consecuencia pudiera afectar el servicio, exponer alguna vulnerabilidad ó en su defecto recomendar la adquisición de soluciones que permitan mitigar los riesgos de los hallazgos identificados.

ANEXOS
DIVISIÓN DE CONTRATOS

- **Planes de mejora y planes de acción.**
    - **TOTALSEC, S.A. DE C.V.**, emitirá recomendaciones al personal operativo o tomadores de decisión para priorizar y llevar a cabo una continuidad en sus mejoras, así como recomendaciones de evaluación periódica para confirmar las mitigaciones.

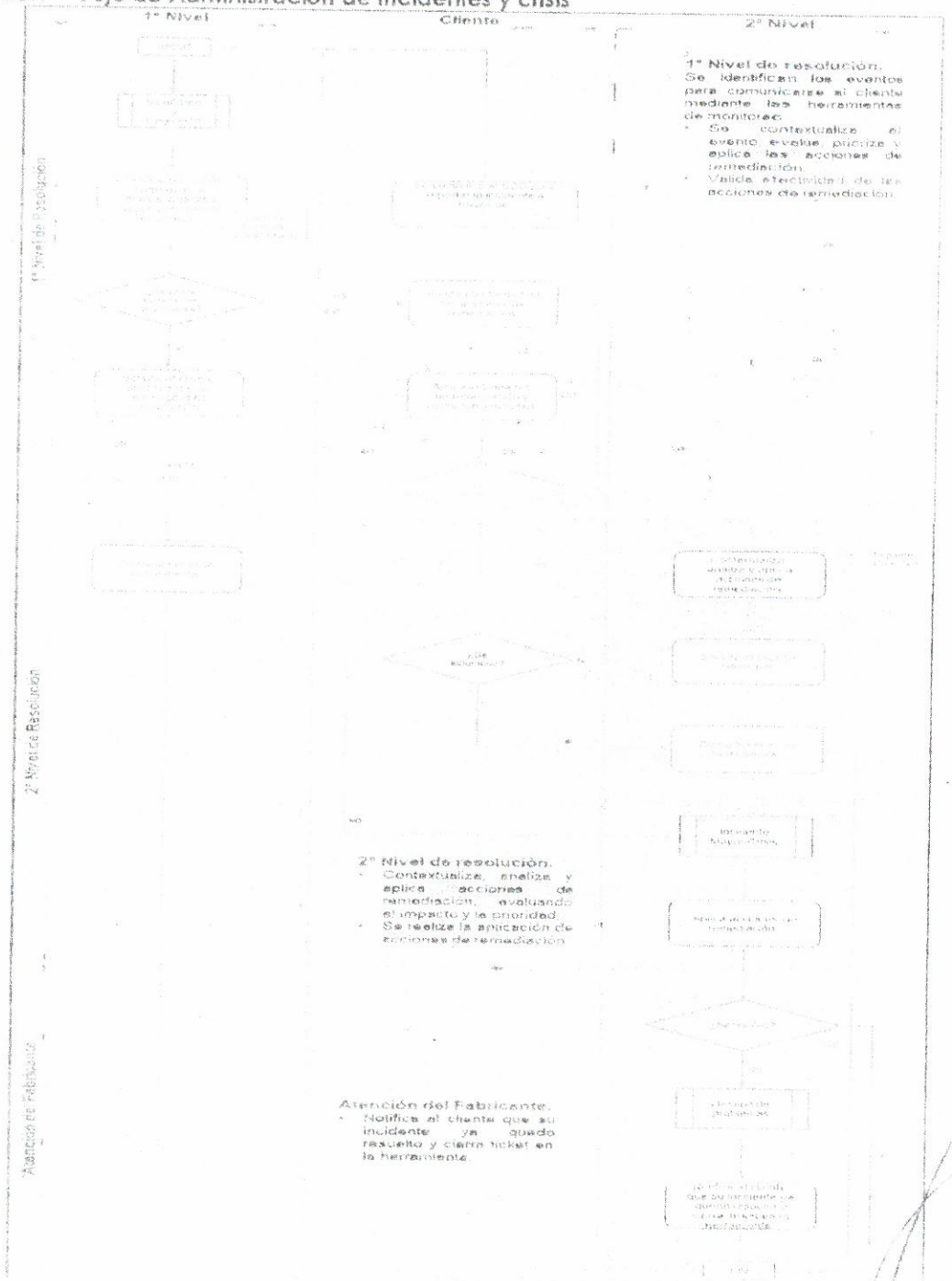
Para dicha actividad **TOTALSEC, S.A. DE C.V.**, se apoyará en herramientas de seguridad propietarias de **TOTALSEC, S.A. DE C.V.**, licenciadas y vigentes, como: la suite de Rapid7.

1.6 Administración de incidentes

TOTALSEC, S.A. DE C.V., asegura que los incidentes de seguridad y TI son gestionados de manera efectiva y eficaz, restableciendo los servicios y herramientas de seguridad en el menor tiempo posible, evitando afectación en la confidencialidad, integridad y disponibilidad de la información.

Todos aquellos incidentes ya sean de TI ó de Seguridad que pertenezcan a los Servicios ofrecidos por **TOTALSEC, S.A. DE C.V.**

1.6.1 Fujo de Administración de incidentes y crisis



ANEXOS
DIVISIÓN DE CONTRATOS

1.6.2 Descripción del ABC de incidentes y crisis

Fase	Actividad	Responsable
1°Nivel	1.Mediante las herramientas de monitoreo identifica un evento y comunica al cliente	SOC
	2. Cliente se comunica para reportar un incidente	Cliente
	3.Contextualiza el evento, valida, prioriza y aplica las acciones de remediación	1° Nivel
Decisión	*¿Requiere actividades adicionales?* SI: Seguir en 4 No: Seguir en 6	
1°Nivel	4. Solicita al cliente aplicar algunas actividades de remediación	SOC
	5. Aplica actividades de remediación y valida funcionalidad	Cliente
	6. Valida efectividad de las acciones de remediación	Cliente
Decisión	*¿Se solucionó?* SI: Seguir en 7 No: Seguir en 8	
2° Nivel	7. Cierra ticket en la herramienta Seguir al FIN	SOC
	8.Se escala el incidente con el 2° Nivel Contextualiza, analiza y aplica acciones de remediación, evaluando el impacto y la prioridad	SOC / 2° Nivel
	9.Solicita al cliente validación	2° Nivel
Decisión	*¿Se solucionó?* SI: Seguir en 10 No: Seguir en 11	

Fase	Actividad	Responsable
2° Nivel	10. Cierra ticket en la herramienta	2° Nivel
	11. Procede a la recategorización del incidente a incidente Mayor y/o Crisis	2° Nivel
	12. Aplica acciones de remediación	2° Nivel
Decisión	*¿Se solucionó?* SI: Seguir en 13 No: Seguir en FIN	
Atención del fabricante	13. Se escala a problema con atención del Fabricante	2° Nivel
	14. Notifica al cliente que su incidente ya quedó resuelto y cierra ticket en la herramienta FIN	2° Nivel

1.7 Administración de problemas

TOTALSEC, S.A. DE C.V., asegura la correcta identificación de los problemas que pudieran afectar la confidencialidad, integridad o disponibilidad de los servicios ofrecidos, con la finalidad de minimizar o evitar el impacto relacionado con problemas, investigando y determinando la causa raíz de los mismos incluyendo su solución.

Todos aquellos problemas que sean identificados mediante el Proceso de Incidentes y Crisis.

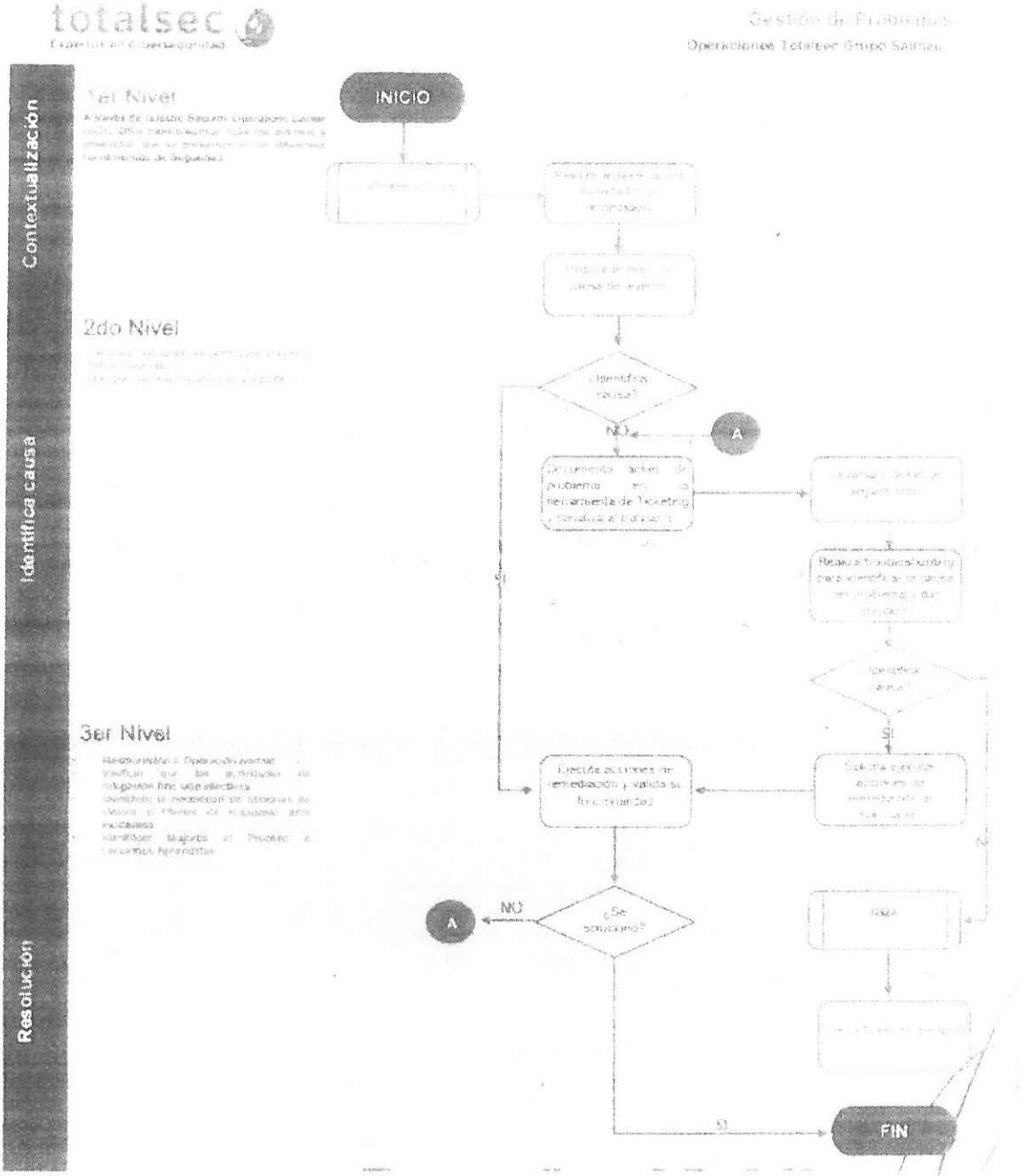
1.7.1 Priorización

Dentro del Proceso de administración de problemas existe la priorización de los mismos, la cual está definida con base al impacto y la urgencia, asignándose de la siguiente manera:

El personal notificará inmediatamente a través de la Mesa de Servicio en el momento que se detecte una falla de los servicios o ante algún incidente de seguridad, indicando la criticidad con la que debe ser atendido considerando lo siguiente.

Prioridad	Descripción
Criticidad Alta	Cuando el servicio no está disponible.
Criticidad Media	Cuando el servicio está disponible y presenta mensajes de error recurrentemente.
Criticidad Baja	Cuando el servicio está disponible y presenta mensajes de error eventuales.

1.7.2 Flujo de Administración de problemas



1.7.3 Descripción del ABC de problemas

Fase	Actividad	Responsable
Contextualización	1.- Da atención a un incidente a través del proceso de gestión de Incidentes.	1° - 2° Nivel de resolución
	2.- Realiza análisis, aplica actividades de remediación.	2° Nivel de resolución
	3.- Realiza análisis de causa del evento	2° Nivel de resolución
Decisión	*¿Identifica causa?* Si: Seguir en 4 No: Seguir en 8	
Identificación de causa	4.- Documenta Ticket de problema en la herramienta de "ticketing" y canaliza con el fabricante	2° Nivel de resolución
	5.- Levanta ticket de seguimiento	Fabricante
	6.- Realiza troubleshooting para identificar la causa del problema y dar solución.	Fabricante
Decisión	*¿Identifica causa?* Si: Seguir en 7 No: Seguir en 8	
Resolución	7.- Solicita ejecutar acciones de remediación al solicitante	Fabricante

ANEXOS
DIVISIÓN DE CONTRATOS

1.8 Investigación de Incidentes

TOTALSEC, S.A. DE C.V., describe las principales actividades durante la fase de Planeación, ejecución y la entrega de los Servicios de Análisis Forense, detallando paso a paso cada una de las actividades a desarrollar.

1.8.1 Objetivo General

Dar continuidad a los servicios de **TOTALSEC, S.A. DE C.V.**, en caso de presentarse una situación de contingencia mayor o catastrófica

1.8.2 Objetivos particulares

a) Este procedimiento se enfoca en la operación en modo contingencia de manera que se puedan minimizar los impactos y dar servicio.
b) Este procedimiento busca coordinar a los equipos de **TOTALSEC, S.A. DE C.V.**, que requieran interactuar en caso de una contingencia
c) Ofrecer respuestas oportunas y apropiadas a cualquier incidente no planeado, reduciendo así el efecto de una interrupción de los servicios de computo.

1.8.3 Los objetivos particulares a considerar son:

- Considerar las actividades especificas para llevar a cabo la ejecución de este servicio.
- Definir los roles, responsabilidades y límites entre las áreas involucradas para la entrega de este servicio.
- Establecer las Políticas para la entrega del Servicio de Análisis Forense.
- Enlazar con los procesos de operación de Totalsec y del Sistema de Gestión que correspondan para la entrega de este servicio.
- Identificar mejoras al servicio.

TOTALSEC, S.A. DE C.V., considera presentar ante el **IMSS** los resultados del análisis sobre la vulneración de alguna aplicación, sitio, equipo, ya sean internos o externos; el desarrollo de esta actividad es un primer paso para la construcción de un programa continuo de mantenimiento de Escaneo de Vulnerabilidades.

TOTALSEC, S.A. DE C.V., tiene como objetivo tengan un panorama acerca de los eventos que pudieron dar lugar al evento de seguridad en cuestión. Este análisis será presentado al **IMSS** con una evaluación realizada por nuestros especialistas calificados, mostrando una revisión de los indicios ofrecidos por el cliente, compartiendo recomendaciones, así como buenas practicas que puedan evitar una reincidencia del suceso.

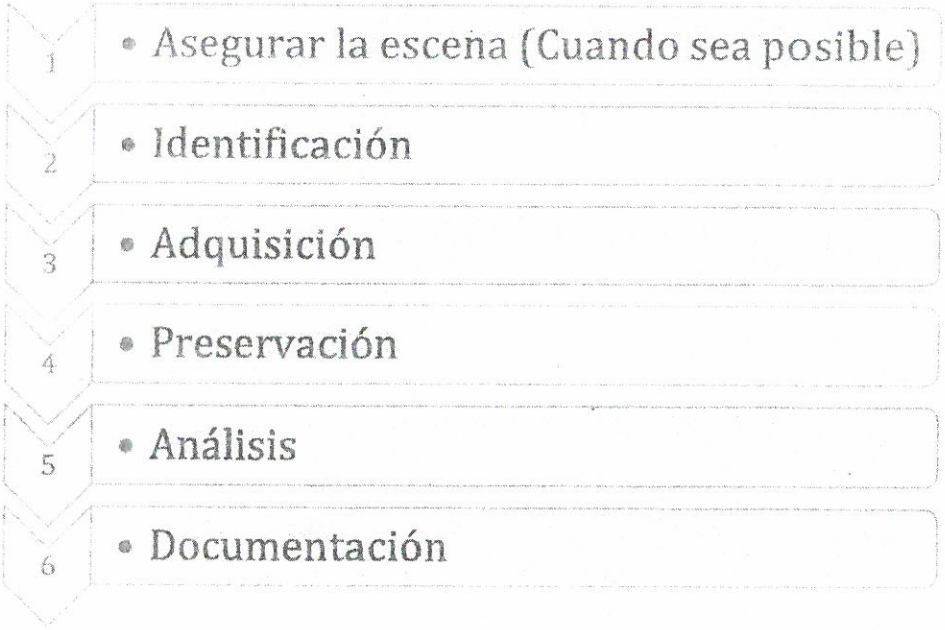
TOTALSEC, S.A. DE C.V., consideramos muy importante la definición de requisitos del Servicio como aquellas actividades y aspectos que deben cumplirse para una entrega y ejecución exitosa del servicio.

Para una ejecución correcta del servicio de Análisis Forense, es necesario cumplir con la siguiente lista de requisitos:

- Disco duro a analizar en formato IMG, vmx, vhdx o el disco duro físico
- Breve descripción de lo ocurrido incluyendo fecha y hora aproximada
- Síntomas o indicios que dan lugar a la sospecha o necesidad del análisis
- Logs de registros del equipo o servicio involucrado

1.8.4 Fases Generales

A continuación, se enumeran las etapas utilizadas en el análisis forense digital



1.8.5 Asegurar la escena

Se trata de la primera fase y no siempre es aplicable, su objetivo es impedir que alguien pueda alterar la evidencia digital

1.8.6 Identificación

TOTALSEC, S.A. DE C.V., pretende identificar qué tipo de incidente o escenario es el que se pretende analizar ya que va de la mano con el proceso de búsqueda y recopilación de evidencias. Antes de comenzar una búsqueda desesperada se debe actuar de forma metódica y profesional ya que lo único que conlleva en una acción desesperada es a una eliminación de "huellas" importantes.

1.8.7 Adquisición

En esta fase **TOTALSEC, S.A. DE C.V.**, obtendrá copias de la información que puede estar vinculada con el incidente. En este punto hay que evitar modificar cualquier tipo de evidencia, para esto se deben utilizar copias bite a bite generadas con las herramientas y dispositivos adecuados. Este tipo de copia nos dejara recuperar archivos borrados o particiones ocultas, arrojando como resultado una imagen de igual tamaño del disco a analizar.

Las evidencias serán rotuladas indicando fecha, hora y deberán ser resguardadas en recipientes que no permitan el deterioro, ni el contacto con el medio, esto para evitar que se puedan corromper o manipular. Esta etapa puede ser complementada con fotografías, con el objetivo de guardar un registro del estado de los equipos y sus componentes electrónicos.

TOTALSEC, S.A. DE C.V., recomendamos utilizar guantes, bolsas antiestáticas y jaulas de Faraday para depositar dispositivos que puedan ser corrompidos por ondas electromagnéticas como son los celulares o discos duros.

1.8.8 Preservación

TOTALSEC, S.A. DE C.V., considera una etapa crítica debido a la posibilidad de modificar por error alguna de las evidencias digitales. Cualquier error puede derivar en invalidar las pruebas en un posible proceso judicial. En esta etapa se debe garantizar la información recopilada, con el fin de que no se destruya o sea modificada. Nunca realizaremos un análisis sobre la muestra original, esta debe hacerse sobre las copias generadas. De este modo, aparece el concepto de cadena de custodia, la cual es un acta en donde se registra el lugar, fecha, analista y demás actores que manipularon la muestra.

TOTALSEC, S.A. DE C.V., utilizar técnicas de Hashes o firma digital para identificar de forma unívoca determinados archivos que podrían ser de gran utilidad para la investigación.

1.8.9 Análisis

TOTALSEC, S.A. DE C.V., lleva a cabo el análisis de las evidencias digitales. La información que se debe analizar principalmente en esta fase es:

- Los registros de los dispositivos IPS y Firewall
- Los registros de logs del sistema operativo y/o servicios

- Estructura de directorios, ficheros que se siguen almacenados, así como los que han sido eliminados, horas y fechas de la creación o modificación de los ficheros, tamaño de los mismos, etc.

1.9 Documentación

TOTALSEC, S.A. DE C.V., finaliza el análisis se debe redactar y presentar un informe de manera clara y sencilla.

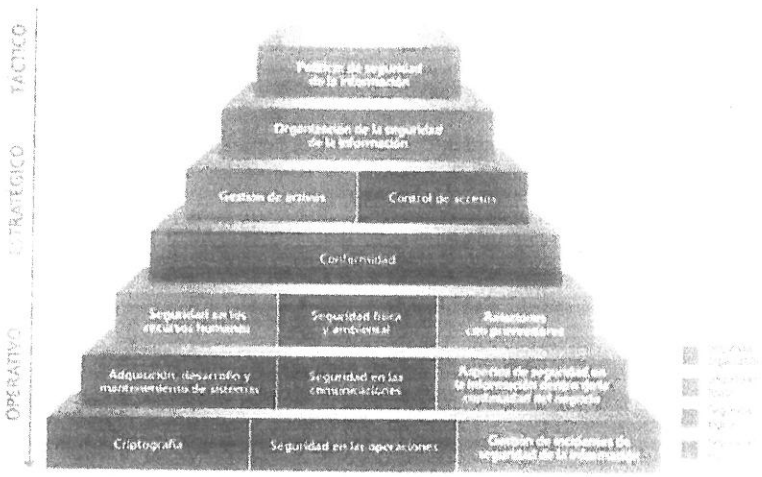
2. Metodología del Sistema de Gestión de la información (SGSI)

TOTALSEC S.A. DE C.V., describe la metodología del SGSI, con el unico objetivo de **presenta como referencia ante el IMSS las capacidades, conocimientos y procedimientos documentados** con los que cuenta **TOTALSEC S.A. de C.V.**, esto en apego al requerimiento del IMSS sobre revisión de los procesos y procedimientos existentes, y no la construcción e implementación de un SGSI, de acuerdo al Servicio de seguridad - Verificación / Calidad, de la investigación de mercado del **SASI-C** del Instituto.

TOTALSEC, S.A. DE C.V., proponer un procedimiento para cumplir con el requerimiento del servicio para el sistema de Gestión y Servicio Administrado de Seguridad de la información bajo la norma ISO/IEC 27001, solicitado por **el instituto**. A continuación, **TOTALSEC, S.A. DE C.V.**, presenta su experiencia en el sistema de gestión, principales regulaciones y normativas

Totalsec

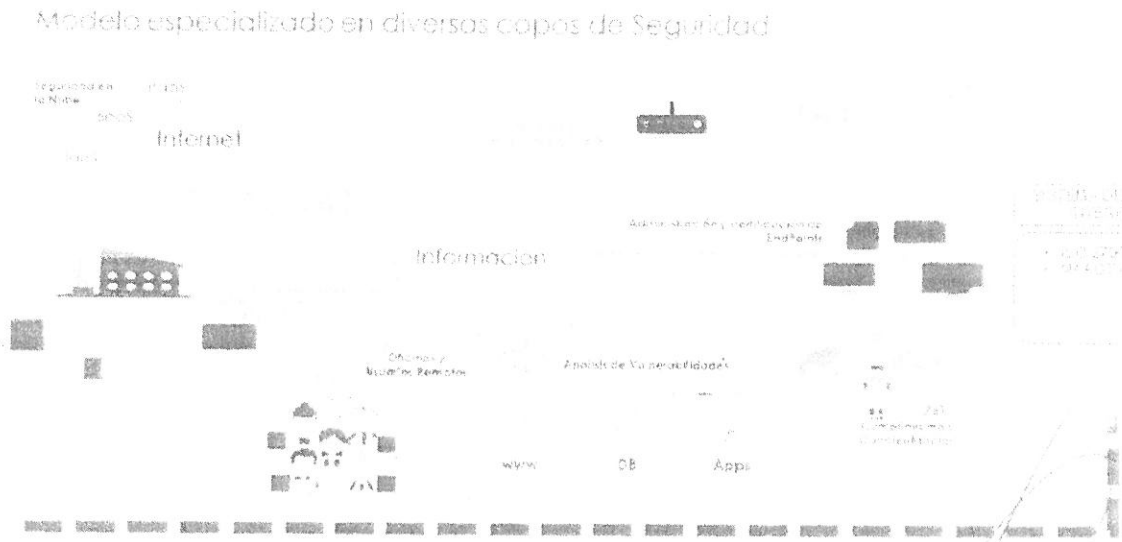
(b) Imagen de consultoría de seguridad de la información



(c) Imagen de los Dominios de la norma ISO 27001:2013

2.1. Entregable A.3: Análisis Institucional

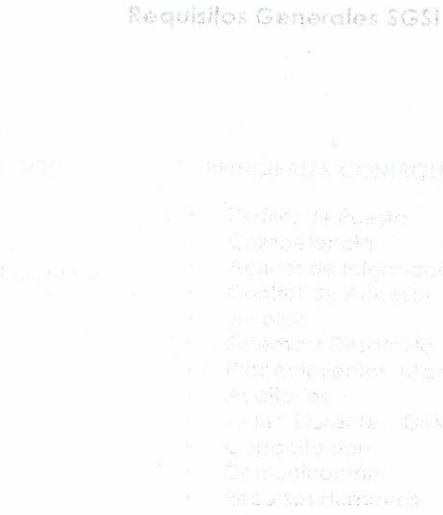
TOTALSEC, S.A. DE C.V., realizará un diagnóstico inicial y documentará la situación institucional en términos de seguridad de la información; y con esto diseñará, a alto nivel, el SGSI del **Instituto**.



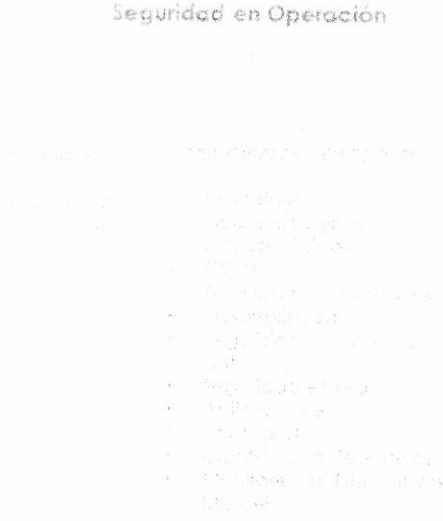
(a) Imagen sistema de gestión de seguridad de la información "modelo conceptual"

2.2 Entregables B.1: analisis del SGSI

TOTALSEC, S.A. DE C.V., realizará un análisis inicial, en las cuales definirá los requisitos y alcanzables para llegar a la correcta implementación del SGSI ante **El Instituto**



(b)Imagen requisitos para análisis de SGSI"



(c)Imagen requisitos para seguridad en operaciones

ANEXOS
DIVISIÓN DE CONTRATOS

2.3 Entregable B.2: Diseño del SGSI

TOTALSEC, S.A. DE C.V., elaborará, presentará, realizará el análisis y la evaluación de riesgos para obtener una priorización basada en niveles de impacto.

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

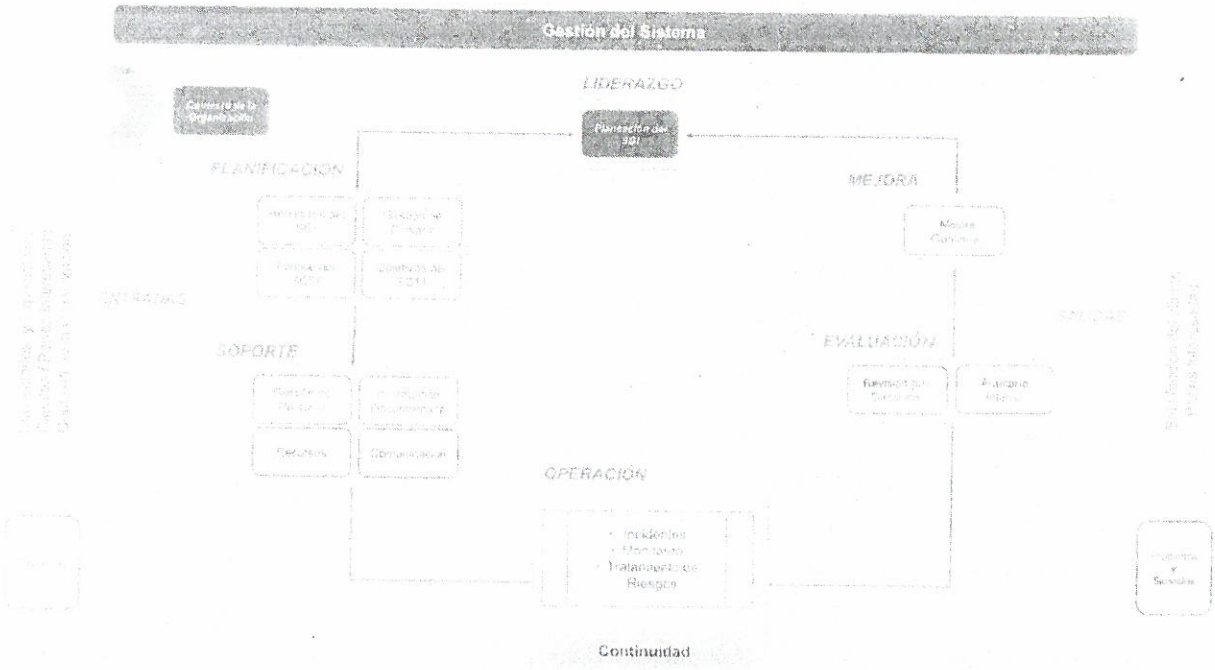
El eje central de ISO 27001 es proteger la CONFIDENCIALIDAD, INTEGRIDAD y DISPONIBILIDAD (CID) de la información en una empresa.

La filosofía principal de la norma ISO 27001 se basa en la Gestión de Riesgos: investigar dónde están los riesgos y luego actuarlos sistemáticamente.

(d)Imagen Gestión de Riesgos

2.4 Entregable 5.3: Construcción del SGSI

TOTALSEC, S.A. DE C.V., realizara la construcción de procesos, procedimientos, formatos y metodología de análisis de riesgos enfocados a la seguridad de información con base en los objetivos y alcance del negocio. Capacitaciones sobre seguridad de la información, así como auditoría interna para garantizar el cumplimiento del estándar ISO 27001.



ANEXOS
DIVISIÓN DE CONTRATOS

3. Continuidad de Operación (Guía DRP)

TOTALSEC S.A DE C.V., describe la metodología del proceso del plan de recuperación en caso de desastre (DRP por sus siglas en ingles), con el único objetivo de presentar como evidencia ante el Instituto las capacidades, conocimientos y procedimientos documentados con la cuenta **TOTALSEC S.A DE C.V.**, misma que servirá para respaldar la experiencia en el desarrollo del proceso de DRP que solicita el Instituto , de acuerdo al punto asociado al inciso (c) Servicios del Centro de Operaciones de Seguridad "SOC", de la investigación de mercado del **SASI-C** para el **Instituto.**

3.1. Objetivo General

El IMSS solicita integrar un plan de recuperación en caso de desastre (DRP por sus sigla en inglés), que integre aquellos servicios de seguridad que resulten críticos para el Instituto, mismo que se definirán en las mesas de trabajo correspondientes, y que tenga el objetivo de trasladar la operación de los presentes servicios a otros centros de datos, pudiendo ser estos del tipo nube privada o nube pública. **TOTALSEC, S.A. DE C.V.**, presenta el proceso para atender una situación de contingencia mayor o catastrófica.

3.2. Objetivos particulares

a) Este procedimiento se enfoca en la operación en modo contingencia de manera que se puedan minimizar los impactos y dar servicio.
b) Este procedimiento busca coordinar a los equipos de **TOTALSEC, S.A. DE C.V.**, que requieran interactuar en caso de una contingencia
c) Ofrecer respuestas oportunas y apropiadas a cualquier incidente no planeado, reduciendo así el efecto de una interrupción de los servicios de computo.

3.3. Roles, Responsabilidades y Autoridades

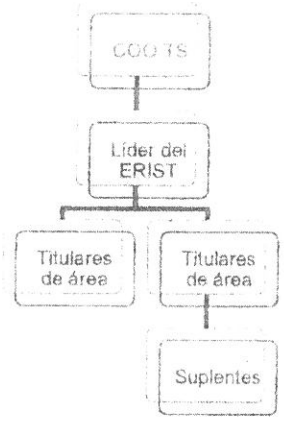
Gestión de Continuidad del Negocio	Responsabilidad
Diseñar y mantener el DRP, identificando a los dueños de los activos críticos para que se apliquen los procedimientos definidos en el plan de recuperación de desastres.	Jefe de área
Diseñar los procesos y los recursos necesarios para reducir al mínimo el impactode la interrupción; asignando responsabilidades.	Jefe de área
Realizar el análisis de impacto al negocio en caso de una interrupción deactividades.	Jefe de área
Garantizar la correcta planificación, desarrollo y el establecimiento de las políticas de continuidad de negocio y los procedimientos para todos los archivos, aplicativos o bases de datos que soporten las funciones esenciales, en las quecontemplen: • Grupos de recuperación • Grupo coordinador • Grupo de Operación • Grupo de comunicaciones	Jefe de área

Gestión de Continuidad del Negocio	Responsabilidad
• Grupo de seguridad Informática	
Establecer todos los procedimientos de recuperación necesarios para dar cumplimiento a las directrices para la recuperación de los procesos críticos encaso de presentarse una indisponibilidad.	Jefe de área
Asegurar los acuerdos contractuales existentes, sobre la base de análisis de impacto, para la continuidad de las actividades de negocio y funciones de los recursos de información, servicios técnicos, en donde se subcontraten serviciosde terceros.	Directiva
Examinar el cumplimiento del Plan de Continuidad de Negocio para validar elcumplimiento de las políticas, normas y directrices.	Jefe de área
Garantizar el desarrollo y la documentación de las estrategias de recuperacióny los procedimientos para funciones críticas de negocio conforme a los SLAs	Directiva
Garantizar que los controles necesarios se siguen durante una emergencia real.	Jefe de área
Dar seguimiento para garantizar el cumplimiento de los resultados.	Directiva
Gestionar un ejercicio de simulacro al menos una vez al año	Jefe de área
Proporcionar los medios necesarios para ofrecer servicios de apoyo técnico, definir y seleccionar en función de costos de recuperación efectiva de estrategias	Jefe de área
Desarrollar y poner en práctica procedimientos adecuados de copias de seguridad y procedimientos de recuperación para todos los datos y software enla instalación.	Jefe de área
Evaluar las funciones de la empresa para identificar los recursos de información (instalaciones, personal, datos, comunicaciones de voz, equipos) necesarios para apoyar la continuidad y la recuperación de los procesos de misión críticaTotalsec	Jefe de área
Identificar, evaluar y disponer la adquisición de otros recursos de información y servicios de recuperación según sea necesario para resaltar las funciones críticas Totalsec	Jefe de área
Verificar que se ejecuta el Plan y Políticas de Continuidad de Negocio.	Directiva
Garantizar que se respeten y mantengan las políticas y procedimientos internos que prevén la continuidad de personal, de la tecnología de la información, instalaciones, software y equipo y las funciones Totalsec.	Jefe de área / Dirección
Garantizar la participación en todos los niveles necesarios para la aplicación del Plan de Continuidad de Negocios y las políticas y procedimientos de recuperación de negocio.	Jefe de área / Dirección
Revisar los resultados obtenidos del ejercicio de simulacro aplicado.	Jefe de área / Dirección

3.4. Políticas de Operación

3.4.1. Estructura de contingencia

Durante la situación de contingencia o crisis, **TOTALSEC, S.A. DE C.V.**, utilizará la siguiente estructura funcional:



3.4.2. Recursos necesarios para la operación en contingencia

Personal		
Descripción	Cantidad	Observación
Titular(es)		
Suplente(s)		
Líder del ERIST		

Posiciones de trabajo del personal			
Modalidad	Descripción	Cantidad	Observación
Home-Office			
Home-Office			

Equipo de Tecnológico		
Descripción	Cantidad	Observación
Software y Aplicaciones		

No.	Nombre	Observación
1		No aplica
2		No aplica
3		No aplica
4		No aplica
6		No aplica
8		No aplica
11		No aplica

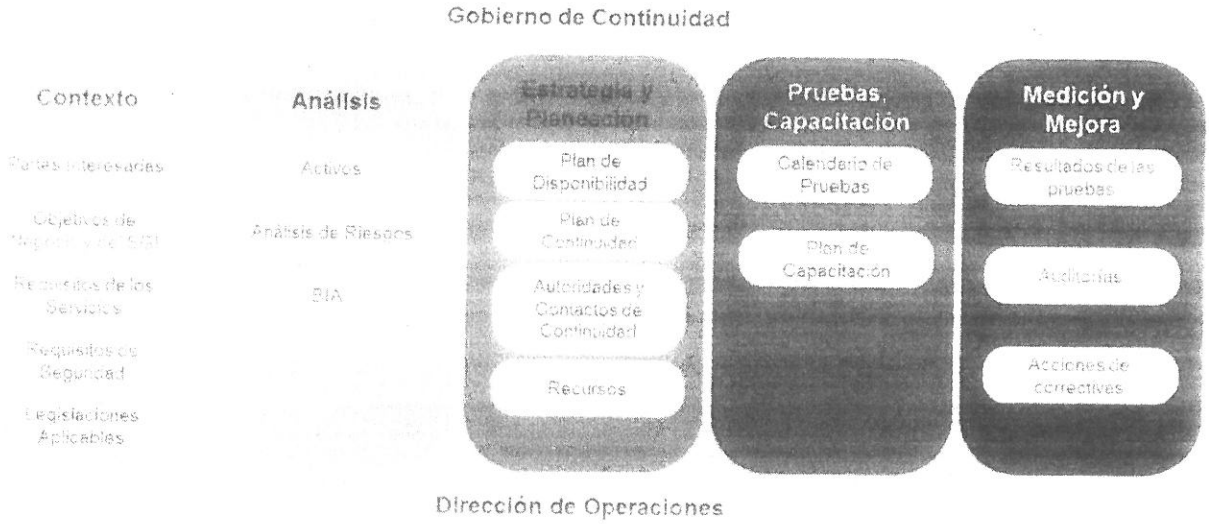
3.4.3.Procesos Críticos

Operación	Antes de 2 horas	Antes de 8 horas	Después de 8 horas
Monitoreo de Ciberseguridad			
Monitoreo de Disponibilidad			
Gestión de Incidentes			
Capacidad de las Tecnologías en Operación			

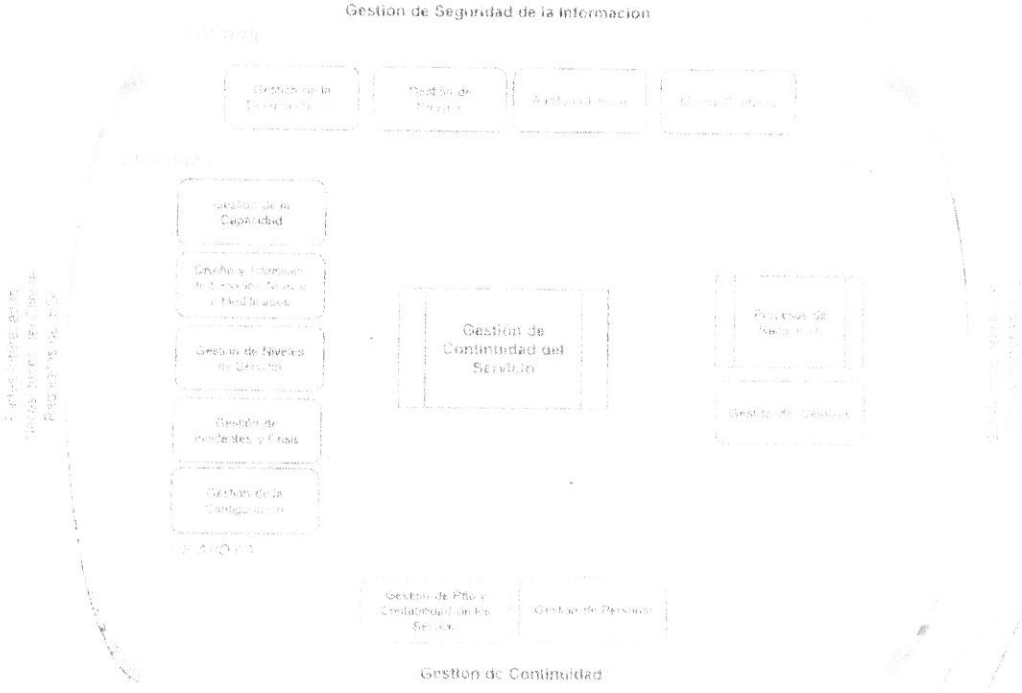
3.4.4.Premisas de la Operación en Contingencia

Para las operaciones críticas de las áreas de Operaciones de TOTALSEC, S.A. DE C.V., considera las siguientes premisas, las cuales deben de cumplirse para poder operar en modo contingencia.

- Contar con la guía de contingencia probada y debidamente actualizada.
- El personal crítico se encuentra debidamente informado del rol a ejecutar durante la contingencia presentada.
- La operación de los procesos críticos de la presente Área Crítica, se debe realizar de acuerdo a las políticas y procedimientos vigentes del área.



3.4.5.Diagramas de Continuidad de servicios



3.4.6.Reconocimiento del evento y su notificación

Una vez que **TOTALSEC, S.A. DE C.V.**, haya identificado y reconocido un evento, el tiempo es vital. Los procedimientos que se presentan a continuación incluyen decisiones que son críticas con respecto al tiempo y que pueden estar basadas únicamente en la magnitud de la contingencia, en su evaluación, y en el impacto de este en las operaciones del negocio.

ANEXOS
DIVISIÓN DE CONTRATOS

3.4.7.Evaluación de los Daños

La evaluación de los daños es la actividad inicial que debe efectuarse inmediatamente después de un incidente, **TOTALSEC, S.A. DE C.V.,** tiene la responsabilidad de investigar y evaluar el incidente, así mismo como comunicarse co otras áreas, para llevar a cabo.

3.4.8.Procedimientos de Respuesta Inmediata

Implementar los procedimientos de respuesta inmediata basados en las circunstancias específicas del evento de acuerdo al Manual de Seguridad del **Insitituto;** Estos procedimientos, normalmente desarrollados por recomendación de Protección Civil, tienen el objetivo de disminuir el impacto al personal, hasta que las condiciones vuelvan a situación normal para los siguientes casos:

- **Notificaciones de Emergencia a Usuarios Finales**

Contactar a los usuarios finales críticos, por medio de un comunicado sobre el incidente.

- **Tareas de los Grupos de Recuperación**

En el momento de declarar un desastre, deberán efectuarse las acciones correspondientes con el objeto de restaurar la infraestructura de cómputo, comunicaciones y las operaciones del personal crítico en el Centro Alterno de Trabajo. Las actividades de estos Grupos en caso de una declaración de desastres.

- **Procedimientos de recuperación de los servicios de cómputo**

El Grupo Coordinador de **TOTALSEC, S.A. DE C.V.,** actúa como una central de control para supervisar la reubicación de recursos disponibles para la recuperación de los servicios del centro de cómputo y apoyar a cualquier usuario en sus requerimientos finales informando al Comité Directivo DRP.

- **Procedimientos para la Declaración de Desastre**

Una vez que el Grupo Coordinador y el Comité Directivo han evaluado el nivel de contingencia y la duración de la interrupción en las operaciones normales de **TOTALSEC, S.A. DE C.V.,** las actividades de Declaración de Desastre y el Desarrollo del Plan de Acción encaminadas a la Recuperación se inician de inmediato. Para declarar un desastre el Grupo Coordinador realiza las siguientes actividades:

  - Recabar la información de diagnóstico y tiempo de recuperación.
  - Analizar el alcance de los daños y si la interrupción a la operación normal del negocio (por fallas de infraestructura tecnológica o la imposibilidad de acceso al edificio de las oficinas corporativas o fallas en las comunicaciones), va a ser mayor a 8 horas, se determina a la declaración del desastre.
  - Notificar telefónicamente a los integrantes de los Grupos de Recuperación.

- Promover una reunión de retro alimentación de información en el Centro de Control de Crisis seleccionado de acuerdo al incidente.
- Solicitar a los líderes de los Grupos de Recuperación iniciar de inmediato la recuperación de acuerdo al Plan.

- **Procedimientos de Restauración**

Las determinaciones para activar los siguientes Procedimientos de Restauración del Centro de Cómputo serán hechos por el Grupo de Recuperación basados en las circunstancias específicas del incidente. El grupo activará personal apropiado para la restauración del Centro de Cómputo dañado. El Grupo de Recuperación supervisará las actividades de planeación e implementación para los Grupos de Recuperación asociados a este punto.

- **Plan de Retorno**

Desarrollar una estrategia de reubicación detallada en el "Plan de Acción de Restauración" para volver a las instalaciones restauradas usando el procedimiento del Plan de Recuperación del Centro de Cómputo como una guía. Después, coordinar el regreso a las instalaciones permanentes (nuevas o reconstruidas) al concluir la operación de recuperación.

3.5 Validación de Indisponibilidad de Instalaciones

El detalle de las actividades a realizar se indica en la siguiente lista de chequeo:

Paso	Responsable	Actividad	Realizado
1.	Líder del ERIST	Recibir la comunicación por parte de la dirección de Operacionesde la activación de la contingencia.	☐
2.	Líder del ERIST	Ejecutar el árbol de llamada correspondiente.	☐
3.	Líder del ERIST	Recibir notificación sobre la estrategia de contingencia a aplicar	☐
4.	Líder del ERIST	¿Se utilizará VPN?**SI:** ir al paso 5 **NO:** ir al paso 7	☐
5.	Líder del ERIST	Definir el lugar en donde se conectarán para la ejecución de lasfunciones.	☐
6.	Líder del ERIST	Notificar al ERIST el tiempo estimado de la reanudación de lasoperaciones. Ir al paso 17.	☐
7.	Líder del ERIST	Verificar si se puede ir a otro sitio a ejecutar las operaciones	☐
8.	Líder del ERIST	¿Hay otro sitio disponible? **SI:** Ir al paso 9 **NO:** ir al paso 19	☐

9.	Líder del ERIST	Recibir la información del sitio	
10.	Líder del ERIST	Indicar el tiempo estimado de llegada al sitio indicado, utilizando aplicaciones de navegación e informarle al ERIST	
11.	Líder del ERIST	Comunicarle al personal no crítico que mientras esté la situación decrisis debe estar pendiente de las comunicaciones oficiales por medio de los canales autorizados.	
12.	Titular	Movilizarse al sitio.	
13.	Titular	Probar los accesos a los sistemas.	
14.	Líder del ERIST	¿Hay problemas de acceso? **SI**: Ir a paso 15 **NO**: ir a paso 18	
15.	Líder del ERIST	Notificar al ERIST la situación presentada.	
16.	Líder del ERIST	Recibir instrucciones sobre cómo proceder por parte de la EquipoERIST.	
17.	Líder del ERIST	Comunicar las instrucciones recibidas al titular.	
18.	Titular	Ejecutar la operación crítica en el lugar alterno. **Fin del procedimiento.**	
19.	Líder del ERIST	Esperar instrucciones sobre cómo proceder de parte del ERIST. **Fin elprocedimiento.**	

3.6 Validación ante Indisponibilidad de Tecnologías

El detalle de las actividades a realizar se indica en la siguiente lista de chequeo:

Paso	Responsable	Actividad	Realizado
1.	Líder del ERIST	Informar a la Equipo ERIST sobre la afectación presentada	
2.	Líder del ERIST	Validar si la interrupción es para todas las operaciones o solamente a algunas.	
3.	Líder del ERIST	¿La interrupción es total? **SI**: ir al paso 7 **NO**: ir al paso 4	
4.	Líder del ERIST	Identificar las operaciones que se están viendo afectadas.	
5.	Líder del ERIST	¿Las operaciones afectadas han sido identificadas como críticas? SI: ir al paso 7	

		NO: ir al paso 6			
6.	Líder del ERIST	Reportar situación a Tecnología como incidente. **Fin del procedimiento.**			
7.	Líder del ERIST	Reportar situación a Tecnología como crisis.			
8.	Líder del ERIST	Monitorear la situación para identificar si se restablecieron los sistemas.			
9.	Líder del ERIST	Esperar indicaciones de la Equipo ERIST. **Fin del procedimiento.**			

3.7 Validación ante Indisponibilidad de Personal

El detalle de las actividades a realizar se indica en la siguiente lista de chequeo:

Paso	Responsable	Actividad	Realizado
1.	Líder del ERIST	Activar el árbol de llamadas para ubicar al personal crítico. *Ver* **¡Error! No se encuentra el origen de la referencia.**	☐
2.	Líder del ERIST	Realizar un inventario del personal crítico disponible para operaren contingencia.	☐
3.	Líder del ERIST	¿Todo el personal titular está disponible? **SI:** Ir a paso 8 **NO:** ir al paso 4	☐
4.	Líder del ERIST	Comunicarse con el personal suplente.	☐
5.	Líder del ERIST	¿El personal suplente está disponible? **SI:** Ir a paso 7 **NO:** Ir al paso 6	☐
6.	Líder del ERIST	Comunicar a Equipo ERIST.	☐
7.	Líder del ERIST	Esperar indicaciones del ERIST. **Fin del procedimiento.**	☐
8.	Líder del ERIST	Operar con el personal disponible en contingencia. **Fin delprocedimiento**	☐

3.8 Validación para la restauración a la Operación normal

A continuación, se indican las acciones a seguir en el retorno a la normalidad para cada uno de los escenarios de indisponibilidad.

Paso	Responsable	Actividad	Realizado
1	Líder del ERIST	Recibir la comunicación por parte de Equipo ERIST sobre el retorno ala normalidad	
2	Líder del ERIST	Comunicar al personal crítico sobre la finalización del trabajo encontingencia	
3	Líder del ERIST	Verificar la conexión utilizada por el VPN	
4	Líder del ERIST	¿El personal está utilizando VPN? **SI:** Ir al paso 12 **NO:** Ir al paso 5	
5	Líder del ERIST	Verificar si se está trabajando con un proveedor alterno	
6	Líder del ERIST	¿Se están utilizando servicios de un proveedor alterno? **SI:** Ir al paso 11 **NO:** Ir al paso 6	
7	Líder del ERIST	Verificar si se están ejecutando las operaciones de forma manual	
8	Líder del ERIST	¿Se están ejecutando las operaciones manualmente? **SI:** Ir al paso 10 **NO:** Ir al paso 9	
9	Líder del ERIST	Comunicar al personal no crítico sobre la finalización del trabajo encontingencia. **Fin del procedimiento**	
1	Líder del ERIST	Recopilar la información generada para su ingreso en los sistemasrespectivos. Ir al paso 9	
1	Líder del ERIST	Comunicarse con el proveedor principal para reanudar la prestaciónde servicios. Ir al paso 7	
1	Líder del ERIST	Solicitar al personal crítico deshabilitar conexión y volver al Sitio Principal	
1	Líder del ERIST	Indicar el tiempo estimado de llegada al sitio principal, e informarle a Unidad de Continuidad de Negocio.	
1	Titular	Deshabilitar la conexión VPN.	
1	Titular	Movilizarse hacia el Sitio Principal. Ir al paso 5.	

3.9 Infraestructura requerida para el proceso

Para este proceso se ocupa como infraestructura:

- El histórico de Pruebas realizadas
- Documentos de Contexto para la organización (FODA, Legislaciones, Objetivos, etc)
- Planes de continuidad anteriores
- BIA (Análisis de Impacto al Negocio)
- Bitácoras de herramientas
- Listado de Personal
- Catálogo de Servicios
- Listado de Procesos y documentos
- Canales de comunicación internos permitidos
- Informes de las pruebas de continuidad

4 Glosario

- **SOC:** Security Operation Center (Centro de Operaciones en Seguridad)
- **CAS:** Centro de atención de Seguridad
- **Ticket:** Herramienta de asignación eventos ó incidentes (Remedy)
- **CMDB:** Configuration Management Data Base (Base de Datos de Gestión de Configuración)
- **CI's:** Configuration Items (Elementos de Configuración)
- **ABC:** Alta, Bajas y Cambios
- **OWASP:** Open Web Application Security Project (Proyecto Abierto de Seguridad en Aplicaciones Web)
- **SGSI:** Sistema de Gestión de la Información

ATENTAMENTE

VÍCTOR RODRÍGUEZ FUENTES
APODERADO LEGAL DE
TOTALSEC, S.A. DE C.V

SIN TEXTO

totalsec
Expertos en Ciberseguridad

Propuesta Económica

Instituto Mexicano del Seguro Social
Dirección de Innovación y Desarrollo Tecnológico (DIDT)
Coordinación de Telecomunicaciones y Seguridad de la Información

A	B	C	D	E	F	G	H					
No.	Descripción de Servicio	Unidad de Medida	Precio Unitario	Cantidad Mínima	Cantidad Máxima	Valor Total Mínimo	Valor Total Máximo	Desempeño	Conexiones simultaneas por seg.	Conexiones nuevas por seg.	Paquetes por seg.	Interfaces 10GbE
	I.- Servicios de Seguridad – Continuidad Operativa											
1	Firewall (Tipo III)	Servicio	$860,000	2	4	$ 1,720,000.00	$ 3,440,000.00	20 Gbps	4,000,000	200,000	3,000,000	12
	II.- Servicios de Seguridad – Verificación y Calidad											
2	Análisis de Vulnerabilidades	Servicio	$3,999.00	90	225	$ 359,910.00	$ 899,775.00	NA	NA	NA	NA	NA
3	Pruebas de Penetración	Servicio	$18,042.00	90	225	$ 1,623,780.00	$ 4,059,450.00	NA	NA	NA	NA	NA
4	Análisis Forense	Servicio	$65,603.00	1	2	$ 65,603.00	$ 131,206.00	NA	NA	NA	NA	NA
5	Borrado Seguro de Información	Servicio	$11,091.00	100	200	$ 1,109,100.00	$ 2,218,200.00	NA	NA	NA	NA	NA
6	Sistema de Gestión de Seguridad de la Información (SGSI)	Servicio	$1,139,207.00	1	1	$ 1,139,207.00	$ 1,139,207.00	NA	NA	NA	NA	NA
7	Gestión de Dominios	Servicio	$21,169.00	1	2	$ 21,169.00	$ 42,338.00	NA	NA	NA	NA	NA
8	Certificados Digitales SSL	Servicio	$34,332.00	4	6	$ 137,328.00	$ 205,992.00	NA	NA	NA	NA	NA
	III.- Servicios de Centro de Operaciones de Seguridad (SOC)											
9	Servicios del Centro de Operaciones de Seguridad (SOC)	Servicio	$47,450,000.00	1	1	$ 47,450,000.00	$ 47,450,000.00	NA	NA	NA	NA	NA
					SUBTOTAL	$ 53,626,097.00	$ 59,586,168.00					
					TOTAL CON IVA	$ 62,206,272.52	$ 69,119,954.88					

INSTRUCCIONES PARA EL LLENADO DE LA SECCIÓN: PRECIOS UNITARIOS

1. El participante deberá indicar como parte de su propuesta económica, los **precios unitarios** que decida otorgar en cada concepto del servicio **escribiéndolos en la columna "D"**. Estos precios unitarios deberán estar **redondeados a dos dígitos decimales (XX.XX)**, deberán ser **mayores a cero** en todos los casos y **no podrán quedar en blanco.**
2. Para determinar el alcance de cada uno de los conceptos mencionados en la columna B, el participante deberá considerar la definición de cada uno de ellos, de acuerdo a lo descrito en el anexo técnico.
3. El archivo **de manera automática indicará en la columna "G" y "H"** las cotizaciones del costo mínimo y máximo de cada concepto de servicio ofertado, atendiendo a sus volumetrías, multiplicando las cantidades de servicio ubicadas en las columnas "E" y "F", por el Precio Unitario ofertado (columna "D") de cada concepto de servicio.
4. La volumetría mínima y máxima que se proporciona en las columnas "E" y "F" es exclusivamente para efectos de cotización y no necesariamente refleja los requerimientos del Instituto, por lo que no se deberá considerar como las cantidades a contratar.
5. El archivo calculará **de manera automática** las suma resultante de la columna "G" y "H" en la celda correspondiente al "TOTAL sin IVA", **indicando el valor de la propuesta económica** del licitante.
7. No se deberá integrar en ningún precio unitario **componentes de costo distintos** a los definidos para dicho servicio en el anexo técnico del proyecto.

Atentamente

Victor Rodríguez Fuentes
Apoderado Legal de Totalsec, S.A. de C.V.

ANEXOS DEL CONTRATO

SIN TEXTO

GOBIERNO DE MÉXICO

IMSS

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

Oficio No. 09 53 84 61 1CFJ/1342/2022

Ciudad de México, a 04 de marzo de 2022.

Asunto: Notificación de Adjudicación

Adjudicación Directa Nacional: **AA-050GYR019-E22-2022**

Recibí original
04 de Marzo 2022
Victor Rodríguez Fuentes

C. Victor Rodríguez Fuentes
Representante Legal de la empresa
Totalsec, S.A. de C.V.
Periférico Sur Número 4121, Col. Fuentes del Pedregal,
Demarcación Territorial Tlalpan, C.P. 14140, Ciudad de México, México.
P r e s e n t e

Mediante oficios números 09 52 17 61 5A00/2022/0037 y 09 52 17 61 5A00/2022/0051 recibidos con fechas 21 de febrero y 03 de marzo de 2022, respectivamente, en la Coordinación de Adquisición de Bienes y Contratación de Servicios, el Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información, solicitó con fundamento en el artículo 41 fracción V de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), la contratación por Adjudicación Directa Nacional de los **Servicios Administrados de Seguridad Informática Continuidad (SASI-C).**

Al respecto, en términos de lo previsto en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos, 3 fracción IX, 26 fracción III, 28 fracción I, 40, 41 fracción V y 47 de la LAASSP, así como 85 de su Reglamento, se le notifica que la citada contratación identificada con el número **AA-050GYR019-E22-2022**, se llevará a cabo con su representada, lo anterior, en virtud de que cumplió con los requisitos legales, técnicos y económicos solicitados, cuya vigencia de la prestación del servicio será a partir del día hábil siguiente a la notificación de la adjudicación y hasta el día 31 de agosto de 2022.

En ese sentido, se le adjudica la prestación de los **Servicios Administrados de Seguridad Informática Continuidad (SASI-C)** por un monto mínimo de **$53,626,097.00 (Cincuenta y tres millones seiscientos veintiséis mil noventa y siete pesos 00/100 M.N.)** y un monto máximo susceptible de ejercerse por **$59,586,168.00 (Cincuenta y nueve millones quinientos ochenta y seis mil ciento sesenta y ocho pesos 00/100 M.N.)**, los montos no incluyen el Impuesto al Valor Agregado (IVA), los cuales se tienen por reproducidos en esta notificación como si a la letra se insertaren.

Con lo dispuesto en los artículos 37, párrafo sexto y 46, primer párrafo de la LAASSP, así como 84 de su Reglamento, con la presente notificación de adjudicación, las obligaciones serán exigibles, sin perjuicio de la obligación de firmar el contrato en la fecha y hora que determine la División de Contratos del Instituto Mexicano del Seguro Social (IMSS o Instituto).

2022 FUERTES

DIVISIÓN DE CONTRATOS

Para efectos de la suscripción del contrato respectivo, es necesario que previamente a su firma, entregue la documentación correspondiente en copia simple y original o copia certificada para cotejo a la División de Contratos, de los siguientes documentos:

a) Acta constitutiva y, en su caso, sus respectivas modificaciones.

b) Poder notarial del representante legal que firmará el contrato.

c) Identificación oficial vigente y con fotografía del representante legal.

d) Cédula de Registro Federal de Contribuyentes.

e) Comprobante de domicilio con vigencia no mayor a 3 meses.

f) En su caso, escrito de estratificación de empresa en términos del artículo 3 de la Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa.

g) Escrito bajo protesta de decir verdad, en términos del artículo 50 y 60 de la LAASSP.

h) Escrito bajo protesta de decir verdad que no desempeña empleo, cargo o comisión en el servicio público o, en su caso, que a pesar de desempeñarlo, con la formalización del contrato correspondiente no se actualiza un conflicto de interés, en términos de la Ley General de Responsabilidades Administrativas.

   En caso de que personas morales, como lo es su representada, dicha manifestación deberá presentarse respecto a los socios o accionistas que ejerza control sobre la sociedad.

i) Opinión positiva de cumplimiento de obligaciones fiscales emitida por el Servicio de Administración Tributaria (SAT) vigente a la firma del contrato, en términos del artículo 32-D del Código Fiscal de la Federación.

j) Opinión positiva de cumplimiento de obligaciones en materia de seguridad social vigente a la firma del contrato emitida por el IMSS, en términos del artículo 32-D del CFF, del Acuerdo ACDO.SA1.HCT.101214/281.P.DIR publicado en el DOF el 27 de febrero de 2015 y del ACDO.AS1.HCT.260220/64.P.DIR publicado en el DOF el 30 de marzo de 2020.

   En caso de que su representada no se encuentre registrada ante este instituto o; cuente con Registro Patronal pero se encuentre dado de baja, de conformidad

con lo dispuesto por el artículo 12 de la Ley del Seguro Social (LSS), no podrá obtener la citada Opinión, por lo cual podrá dar cumplimiento a tal requerimiento presentando lo siguiente:

I. Documento emitido por este Instituto (resultado de la consulta en el sistema para obtener la Opinión), en el que se haga constar que no se puede emitir la Opinión de cumplimiento, de conformidad con la Regla Quinta del Anexo único del ACDO.AS1.HCT.260220/64.P.DIR publicado en el DOF el 30 de marzo de 2020.

II. Escrito libre, bajo protesta de decir verdad, que no le es posible obtener la multicitada Opinión, justificando el motivo y anexando el documento en el que conste que no se puede emitir la misma, y

En el caso de aquellos patrones (proveedores o contratistas y sus subcontratados) que tengan más de un Registro Patronal ante el Instituto y alguno o más de uno de estos Registros no se encuentre al corriente en el cumplimiento de las multicitadas obligaciones, no se podrá considerar que se encuentra al corriente en el cumplimiento de dichas obligaciones, aun cuando el registro patronal que haya utilizado para el contrato que se trate si se encuentre al corriente en sus pagos, por lo que deberá regularizar todos sus Registros a efecto de poder obtener la Opinión positiva.

En caso de que su representada se encuentre inscrita, en el Registro Único de Proveedores y Contratistas de CompraNet, deberá remitir únicamente la documentación referida en los incisos: g), h) i), j) y k).

k) Constancia vigente de situación fiscal emitida por el Instituto del Fondo Nacional de la Vivienda para los Trabajadores (INFONAVIT), en los términos establecidos por las "Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de amortizaciones" publicadas en el Diario Oficial de la Federación (DOF) el 28 de junio del 2017.

El IMSS se reserva el derecho de firmar el contrato si no presenta las Opiniones positivas emitidas por el SAT e IMSS, o no acredita estar al corriente en el pago de aportaciones patronales y entero de descuentos ante el INFONAVIT, documentos indispensables para la firma del contrato. En caso de no presentarlos, se procederá a informar al Órgano Interno de Control del Instituto, la no formalización del contrato por causas imputables al proveedor para que determine, en su caso, la sanción correspondiente.

Asimismo, de conformidad con el artículo 48 de la LAASSP se informa a la empresa adjudicada que deberán entregar la Garantía de Cumplimiento de Contrato dentro de los 10 (diez) días naturales posteriores a la firma del mismo.

A fin de que el Área Contratante esté en condiciones de incorporar al Sistema CompraNet los datos relativos al contrato que se derive de este procedimiento de contratación, su representada es responsable de estar inscrita y mantener actualizada su información en el Registro Único de Proveedores y Contratistas (RUPC) de CompraNet; de conformidad y para los efectos de lo establecido en las disposiciones 18 y 19 del "*Acuerdo por el que se establecen las disposiciones que deberán observar para la utilización del Sistema Electrónico de Información Pública Gubernamental denominado CompraNet*", publicado en el Diario Oficial de la Federación el 28 de junio de 2011.

La firma del contrato se realizará dentro de los 15 (quince) días naturales posteriores a la presente notificación de adjudicación en la División de Contratos, sita en la Calle de Durango número 291, Piso 10, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, Ciudad de México, lo anterior, de conformidad a lo establecido en el artículo 46 de la LAASSP.

Lo anterior, se comunica de conformidad con el artículo 2, fracción I del Reglamento de la LAASSP; numeral 4.2.4.1.3 del Manual Administrativo de aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público, 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 y numeral 7.1.3.1.2.3 del Manual de Organización de la Dirección de Administración del Instituto.

Sin más por el momento, aprovecho la oportunidad para enviar un cordial saludo.

Atentamente

Mtra. Elia Sandra Varas Galeana
Titular de la División

Con copia para:
Mtra. María Gabriela Quintanar Olvera.-Titular de la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos. Presente. (*)
(*) Se envía copia por SICGC.

ADJUDICACIÓN DIRECTA NACIONAL AA-050GYR019-E22-2022
SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA CONTINUIDAD (SASI-C)

En la Ciudad de México, siendo las **17:00** horas del día **04 de marzo de 2022**, en las oficinas de la División de Contratación de Activos y Logística, ubicadas en la Calle de Durango Número 291, quinto piso, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, Ciudad de México; se reunieron los servidores públicos cuyos nombres y firmas aparecen al final de la presente acta, con objeto de llevar a cabo la Adjudicación Directa Nacional Número **AA-050GYR019-E22-2022**, para la contratación de los **Servicios Administrados de Seguridad Informática Continuidad (SASI-C)**.----------

----------**Adjudicación** ----------

De conformidad con el artículo 37 fracción VI de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante LAASSP), el presente acto es presidido por la Mtra. Elia Sandra Varas Galeana, Titular de la División de Contratación de Activos y Logística, adscrita a la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos dependiente de la Coordinación de Adquisición de Bienes y Contratación de Servicios, de conformidad con el numeral 5.3.8 inciso a) de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios (en adelante POBALINES) del Instituto Mexicano del Seguro Social (en adelante el IMSS o el Instituto), en correlación con el numeral 7.1.3.1.2.3 del Manual de Organización de la Dirección de Administración, servidora pública facultada para presidir el presente evento.----------

Con fundamento en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos, 26 fracción III, 28 fracción I, 40, 41 fracción V y 47 de la LAASSP, así como el artículo 85 de su Reglamento (en adelante RLAASSP), las POBALINES y demás disposiciones aplicables en la materia, la División de Contratación de Activos y Logística, lleva a cabo la Adjudicación Directa Nacional **AA-050GYR019-E22-2022**, para la contratación de los **Servicios Administrados de Seguridad Informática Continuidad (SASI-C)**. ----------

Atendiendo a lo anterior, con fundamento en los artículos 40, 41 fracción V y 47 de la LAASSP, así como 85 del RLAASSP, se notifica la adjudicación de los **Servicios Administrados de Seguridad Informática Continuidad (SASI-C)**, adjudicación **dictaminada como procedente por el Área Requirente**, en términos de lo previsto por el antepenúltimo párrafo del artículo 41 de la LAASSP, de la siguiente manera: ----------

Empresa: **Totalsec, S.A. de C.V.** ----------

Partida	Nombre	Monto mínimo antes de IVA	Monto máximo antes de IVA
Única	**Servicios Administrados de Seguridad Informática Continuidad (SASI-C)**	**$53,626,097.00 (Cincuenta y tres millones seiscientos veintiséis mil noventa y siete pesos 00/100 M.N.)**	**$59,586,168.00 (Cincuenta y nueve millones quinientos ochenta y seis mil ciento sesenta y ocho pesos 00/100 M.N.)**

ADJUDICACIÓN DIRECTA NACIONAL AA-050GYR019-E22-2022
SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA CONTINUIDAD (SASI-C)

Considerando que de esta forma se aseguran las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes para el Instituto. ----------

Se verificó en CompraNet en la liga https://directoriosancionados.funcionpublica.gob.mx/sanfictec/jsp/ficha_tecnica/sancionadosn.htm que **la empresa antes mencionada no se encuentra inhabilitada y/o sancionada** a la fecha de celebración del presente Acto, se imprimió el directorio correspondiente, mismo que se encuentra archivado en el expediente del procedimiento de la presente adjudicación.----------

Asimismo, **se consultó el listado de proveedores y contratistas impedidos** para contratar con el Instituto Mexicano del Seguro Social, de conformidad con lo establecido por el artículo 50 de la LAASSP, fracciones III, IV, XIII y XIV, dicho listado fue impreso y, de igual manera, se encuentra archivado en el expediente de la presente adjudicación, verificándose que **el cotizante referido no se encuentra impedido**.----------

El monto adjudicado es por un monto mínimo de **$53,626,097.00 (Cincuenta y tres millones seiscientos veintiséis mil noventa y siete pesos 00/100 M.N.)** y un monto máximo de **$59,586,168.00 (Cincuenta y nueve millones quinientos ochenta y seis mil ciento sesenta y ocho pesos 00/100 M.N.)** los montos no incluyen el Impuesto al Valor Agregado (IVA), de acuerdo a la oferta presentada por la empresa adjudicada en su propuesta económica. ----------

El Servicio deberá prestarse de conformidad con el Anexo Técnico y los Términos y Condiciones emitidos por el Área Requirente y Técnica que rige la presente contratación. ----------

La vigencia de la contratación será conforme a lo señalado en los Términos y Condiciones. ----------

De conformidad con el artículo 48 de la LAASSP se le informa al proveedor adjudicado que deberá entregar la Garantía de Cumplimiento de Contrato dentro de los 10 (diez) días naturales posteriores a la firma del contrato correspondiente. ----------

De conformidad con el artículo 37 fracción V de la LAASSP se le informa a la empresa **Totalsec, S.A. de C.V.**, que respecto con lo establecido en el artículo 46 de la LAASSP, la firma del contrato se realizará dentro de los 15 (quince) días naturales siguientes a la presente adjudicación, en la División de Contratos, ubicada en la Calle de Durango No. 291, Décimo Piso, Colonia Roma Norte, Código Postal 06700, Demarcación Territorial Cuauhtémoc, Ciudad de México, en días y horas hábiles con un horario de 09:30 a 14:00 y de 16:00 a 18:00 horas, para lo cual **previamente** deberán entregar en esa División de

ADJUDICACIÓN DIRECTA NACIONAL AA-050GYR019-E22-2022
SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA CONTINUIDAD (SASI-C)

Contratos copia y original para cotejo de los siguientes documentos:----------

Persona moral: ----------

a. Acta constitutiva y, en su caso, sus respectivas modificaciones. ----------

b. Poder notarial del representante legal que firmará el contrato. ----------

Persona física: ----------

a. Acta de nacimiento o carta de naturalización. ----------

Ambos: ----------

a) Identificación oficial vigente y con fotografía del representante legal (cartilla del servicio militar nacional, pasaporte, credencial para votar o cédula profesional), tratándose de personas físicas, y en el caso de personas morales, de la persona que firme la propuesta. ----------

b) Cédula de Registro Federal de Contribuyentes.----------

c) Comprobante de domicilio con vigencia no mayor a 3 meses.----------

d) En su caso, escrito de estratificación de empresa en términos del artículo 3 de la Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa.----------

e) Escrito bajo protesta de decir verdad, en términos del artículo 50 y 60 de la LAASSP.----------

f) Opinión positiva de cumplimiento de obligaciones fiscales emitida por el SAT, vigente a la firma del contrato, en términos del artículo 32-D del Código Fiscal de la Federación.----------

g) Opinión positiva de cumplimiento de obligaciones fiscales en materia de seguridad social vigente a la firma del contrato emitida por el Instituto Mexicano del Seguro Social (IMSS), en términos del artículo 32-D del Código Fiscal de la Federación y del Acuerdo ACDO.SA1.HCT.101214/281.P.DIR dictado por el H. Consejo Técnico de "EL INSTITUTO" publicado en el Diario Oficial de la Federación el 27 de febrero de 2015 y su modificación de fecha 30 de marzo de 2020.----------

h) Escrito bajo protesta de decir verdad que no desempeña empleo, cargo o comisión en el servicio público o, en su caso, que a pesar de desempeñarlo, con la

ANEXOS
2022
DIVISIÓN DE CONTRATOS

formalización del contrato correspondiente no se actualiza un conflicto de interés. (Artículo 49 fracción IX de la Ley General de Responsabilidades Administrativas DOF 18-07-2016). ----------

i) Constancia de situación fiscal vigente, emitida por el Instituto del Fondo Nacional de la Vivienda para los Trabajadores (INFONAVIT) en los términos establecidos por las "Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de amortizaciones" publicadas en el Diario Oficial de la Federación (DOF) el 28 de junio del 2017.----------

El proveedor autoriza al IMSS consultar en tiempo real y en línea, la opinión de cumplimiento en materia de contribuciones de seguridad social, a través de los sistemas electrónicos que para tales efectos dispone la Dirección de Incorporación y Recaudación del IMSS. ----------

En caso de que el proveedor adjudicado haya participado en proposición conjunta, los documentos señalados deberán presentarse por cada uno de los integrantes del consorcio.----------

En caso de que el proveedor: ----------

I. No se encuentre registrado ante este instituto o;----------

II. Cuente con Registro Patronal pero se encuentre dado de baja o;----------

III. No tenga personal que sea sujeto de aseguramiento obligatorio, de conformidad con lo dispuesto por el artículo 12 de la Ley del Seguro Social (LSS).----------

No podrá obtener la citada Opinión, por lo cual dicho proveedor podrá dar cumplimiento a tal requerimiento presentando lo siguiente: ----------

i. Documento emitido por este Instituto (resultado de la consulta en el sistema para obtener la Opinión), en el que se haga constar que no se puede emitir la Opinión de cumplimiento, de conformidad con la Regla Quinta del Anexo único del ACDO.AS1.HCT.260220/64.P.DIR dictado por el H. Consejo Técnico de "EL INSTITUTO" publicado en el Diario Oficial de la Federación el 30 de marzo de 2020;----------

ii. Escrito libre, bajo protesta de decir verdad, que no le es posible obtener la multicitada Opinión, justificando el motivo y anexando el documento en el que conste que no se puede emitir la misma y;----------

ADJUDICACIÓN DIRECTA NACIONAL AA-050GYR019-E22-2022
SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA CONTINUIDAD (SASI-C)

En el caso de que el proveedor manifieste que presta sus servicios a través de trabajadores subcontratados con un tercero, deberá de presentar en tal caso, junto con la documentación citada en los dos párrafos anteriores, la Opinión de cumplimiento de obligaciones del subcontratante, desde luego, vigente y positiva (lo anterior en términos del artículo 15-A de la LSS).----------

En caso de que el participante forme parte de un grupo comercial y uno de los entes que forma parte del grupo se encarga de administrar la plantilla laboral de todas las empresas que lo conforman, será necesario que exhiba el documento que acredite la subcontratación para situarse en el supuesto del párrafo anterior.----------

En caso de que el proveedor no cuente con trabajadores debido a que celebró contrato de prestación de servicios con otra empresa que es la que tiene contratados a los trabajadores (outsourcing), deberá presentar dicho contrato, así como escrito libre en el que manifieste que no se encuentra obligado debido a tal situación y opinión positiva vigente de cumplimiento de obligaciones en materia de seguridad social de la empresa subcontratada emitida por el IMSS.----------

En caso de que el proveedor no cuente con trabajadores, deberá presentar escrito libre en el que manifieste que no se encuentra obligado a inscribirse ante el IMSS, por lo que no puede obtener la opinión de cumplimiento de obligaciones en materia de seguridad social. ----------

Para los casos de contratos que se formalicen con personas físicas que presten sus servicios por sí mismos y por lo tanto no cuentan con un Registro Patronal ni tengan trabajadores registrados en el Instituto, el particular deberá de manifestar mediante escrito libre, bajo protesta de decir verdad, que no le es posible obtener la multicitada Opinión, justificando el motivo y anexando el documento (resultado de la solicitud de Opinión que le da el Sistema institucional) en el que conste que no se puede emitir la misma.----------

En el caso de aquellos patrones (proveedores o contratistas y sus subcontratados) que tengan más de un Registro Patronal ante el Instituto y alguno o más de uno de estos Registros no se encuentre al corriente en el cumplimiento de las multicitadas obligaciones, no se podrá considerar que se encuentra al corriente en el cumplimiento de dichas obligaciones, aun cuando el registro patronal que haya utilizado para el contrato que se trate si se encuentre al corriente en sus pagos, por lo que deberá regularizar todos sus Registros a efecto de poder obtener la Opinión positiva.----------

En caso de que el participante cuente con trabajadores contratados bajo el régimen de honorarios asimilados a salarios, deberá presentar el(los) contrato(s) con los que acredite el régimen de contratación, así como escrito libre en el que manifieste que no se encuentra obligado a inscribirse ante el IMSS debido a tal situación, por lo que no puede

obtener la opinión de cumplimiento de obligaciones en materia de seguridad social.------

Para efectos de lo anterior, el proveedor deberá presentar un escrito en el que manifieste bajo protesta de decir verdad si se encuentra o no subcontratando algún servicio u obra especializada para llevar a cabo sus operaciones cotidianas, en el cumplimiento de su objeto social o para la prestación de servicios y/o enajenación de bienes que pretende realizar en favor del IMSS.----------

En caso de que el proveedor se encuentre inscrito en el Registro Único de Proveedores y Contratistas de CompraNet, deberá remitir únicamente la documentación referida en los incisos: **f), g), h) i).**----------

De conformidad con lo dispuesto en el artículo 37 Bis de la LAASSP, se fijará una copia de la presente acta, en el tablero de comunicación de la División de Contratación de Activos y Logística, situada en la Calle de Durango Número 291, quinto piso, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, Ciudad de México, por un plazo no menor a 5 (cinco) días hábiles, por lo que es de exclusiva responsabilidad de los participantes, acudir a enterarse de su contenido y obtener copia de la misma. ----------

---------- **Cierre del Acta**----------

No existiendo otro asunto que tratar, se da por terminado este acto, siendo las **17:30 horas**, del día de su inicio, esta acta consta de **6 (seis) hojas**, firmando para los efectos **legales procedentes y de conformidad por los asistentes a este acto, quienes reciben copia de la misma**----------

Por el IMSS:----------

Cargo o Representación	Nombre y firma
Titular de la División de Contratación de Activos y Logística (Área Contratante)	Mtra. Elia Sandra Varas Galeana

----------FIN DE TEXTO----------

GOBIERNO DE MÉXICO

IMSS

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

ATENTA NOTA

Ciudad de México, a 15 de marzo de 2022.

Lic. Humberto Rincón Juárez
Titular de la División de Contratos
P r e s e n t e

Por medio de la presente, me permito remitir copia simple de la Atenta Nota 008 signada por el Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información, misma que contiene las aclaraciones solicitadas por esa División de Contratos, a efecto de continuar con la formalización de contrato derivado del procedimiento de Adjudicación Directa Nacional Número **AA-050GYR019-E22-2022** para la contratación de los **Servicios Administrados de Seguridad Informática Continuidad (SASI-C)**.

Lo anterior, para los efectos legales y administrativos a los que haya lugar.

Sin más por el momento, reciba un cordial saludo.

A t e n t a m e n t e

Mtra. Elia Sandra Varas Galeana
Titular de la División

INSTITUTO MEXICANO DEL SEGURO SOCIAL
COORDINACIÓN TÉCNICA DE PLANEACIÓN
15 MAR 2022
RECIBIDO
DIVISIÓN DE CONTRATOS

Elaboró

Lic. Angela Abigail Cruz Cedillo
Jefe Div Operativa E0

ANEXOS
DIVISIÓN DE CONTRATOS

Ciudad de México, a 15 de marzo de 2022.

ATENTA NOTA 008

Mtra. Elia Sandra Varas Galeana
Titular de la División de Contratación de Activos y Logística
Presente

Me refiero al correo electrónico de fecha 15 de marzo del presente año, mediante el cual se solicitaron aclaraciones en nuestro carácter de Área Requirente y Técnica dentro del procedimiento número **AA-050GYR019-E22-2022** para la contratación de los **Servicios Administrados de Seguridad Informática Continuidad (SASI-C)**, en términos de las observaciones efectuadas por la División de Contratos.

Sobre el particular, me permito efectuar las aclaraciones que se mencionan a continuación:

- La Garantía de Cumplimiento de Contrato referida en la página 7 de 54 del numeral 8. GARANTÍAS de los Términos y Condiciones del servicio que nos ocupa, se entregará dentro de los 10 (diez) días naturales posteriores a la firma del contrato correspondiente, en concordancia con el Acta de Adjudicación y Oficio de Notificación de Adjudicación, ambos de fecha 04 de marzo de 2022.

- La persona servidora pública con quién se llevará a cabo el Convenio de Confidencialidad y Resguardo de Información, referido en la página51 de 54 numeral 14. CONVENIO DE CONFIDENCIALIDAD Y RESGUARDO DE LA INFORMACIÓN, será la persona designada como Administradora de Contrato, en términos del oficio número 09 52 17 61 5A00/2022/0025 de fecha 31 de enero de 2022.

Sin más por el momento, reciba un cordial saludo.

INSTITUTO MEXICANO DEL SEGURO SOCIAL
COORDINACIÓN TÉCNICA DE ADQUISICIÓN DE BIENES DE INVERSIÓN Y ACTIVOS
15 MAR 2022
CONTRATACION

Atentamente,

Lic. Fernando González Velázquez
Coordinador de Telecomunicaciones y Seguridad de la Información
Adscrito a la DIDT

IMSS	INSTITUTO MEXICANO DEL SEGURO SOCIAL DIRECCIÓN DE ADMINISTRACIÓN UNIDAD DE ADQUISICIONES COORDINACIÓN DE ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS COORDINACIÓN TÉCNICA DE PLANEACIÓN Y CONTRATOS	Contrato Número S2M0038

ANEXO 3 (TRES)

"DOCUMENTO DE DESIGNACIÓN DE ADMINISTRADOR DEL CONTRATO"

EL PRESENTE ANEXO CONSTA DE **02** HOJAS INCLUYENDO ESTA CARÁTULA

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

Of Nº 09 52 17 61 5A00/2022/0025

Ciudad de México, a 31 de enero de 2022

Ing. Abraham Gutiérrez Castillo
Titular de la División de Seguridad
Informática Física
P r e s e n t e

Me refiero al procedimiento de contratación del ***"Servicio Administrado de Seguridad Informática Continuidad (SASI-C)"***, con fecha de inicio a partir del día hábil siguiente a la notificación de la adjudicación y terminación el 31 de agosto de 2022.

Al respecto y a efecto de atender de manera oportuna las necesidades en materia de Tecnología de la Información y Comunicaciones del Instituto Mexicano del Seguro Social, le informo que esa División a su cargo, ha sido designada para fungir como área técnica y Usted como administrador del contrato, con fundamento en lo dispuesto por los artículos 2, fracción V, 74, y 84 del Reglamento Interior del Instituto Mexicano del Seguro Social 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, lo exhorto a desempeñar los cargos que le han sido conferidos y que se formalizarán 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 enviarle un cordial saludo.

Atentamente

Lic. Fernando González Velázquez
Titular de la Coordinación de Telecomunicaciones y
Seguridad de la Información

RYM 16:22

FGV/COVV/jom

SIN TEXTO