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 (SASI) 2025", (PARTIDA 1),** QUE CELEBRAN, POR UNA PARTE, EL INSTITUTO MEXICANO DEL SEGURO SOCIAL, EN LO SUCESIVO **"EL INSTITUTO",** REPRESENTADO POR LA **C. ELIA SANDRA VARAS GALEANA,** EN SU CARÁCTER DE **TITULAR DE LA COORDINACIÓN TÉCNICA DE ADQUISICIÓN DE BIENES DE INVERSIÓN Y ACTIVOS Y APODERADA LEGAL,** Y POR LA OTRA, LA EMPRESA DENOMINADA **OPERBES, S.A. DE C.V.,** EN LO SUCESIVO **"EL PROVEEDOR"**, REPRESENTADA POR LOS **C.C. LUIS ALBERTO DE LA GARZA AGUIRRE Y LUIS RENE LALIEU REYGADAS**, EN SU CARÁCTER DE REPRESENTANTE LEGAL, A QUIENES DE MANERA CONJUNTA SE LES DENOMINARÁ **"LAS PARTES"**, AL TENOR DE LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

DECLARACIONES

I. "EL INSTITUTO" declara que:

I.1 "EL INSTITUTO" 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 Conforme a lo dispuesto por el artículo 268 A de la Ley de Seguro Social, acredita su personalidad mediante el testimonio de la Escritura Pública número 45,902 de fecha 25 de julio de 2023, otorgada ante la fe del Licenciado José Luis Franco Varela, Titular de la Notaría Pública Número 150 de la Ciudad de México, en cuyo protocolo también actúa por convenio de asociación, el Licenciado José Luis Franco Jiménez, Titular de la Notaría 64 de la Ciudad de México, e inscrita en el Registro Público de Organismos Descentralizados bajo el folio número 97-7-28072023-130615, de fecha 28 de julio de 2023; 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, la **Mtra. Elia Sandra Varas Galeana**, Titular de la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos y Apoderada Legal con **R.F.C.** [redacted], es una servidora pública adscrita a la misma que cuenta con facultades legales para celebrar el presente contrato, quien podrá ser sustituida en cualquier momento en su cargo o funciones, sin que por ello, sea necesario celebrar un convenio modificatorio.

I.3 De conformidad con el artículo 84, penúltimo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"LAASSP"**, suscribe el presente instrumento el **C. Javier Cortés López**, **Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información,** con R.F.C. [redacted] quien lo hace en el siguiente carácter:

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: RFC, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

A) Administrador del presente contrato en cuyo caso en el **Anexo 4 (cuatro)** se encuentra la designación correspondiente.

En todo caso, el administrador o los administradores de presente contrato son las personas servidoras públicas responsables de dar seguimiento y verificar el cumplimiento de los derechos y obligaciones establecidos en este instrumento jurídico, de conformidad con lo dispuesto en los artículos 2, fracción III Bis y 84, penúltimo párrafo del Reglamento de la **"LAASSP"**.

I.4 La adjudicación del presente contrato se realizó mediante el procedimiento de Adjudicación Directa Electrónica de carácter Nacional, número **AA-50-GYR-050GYR019-N-157-2025,** al amparo de lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 6 fracción IX, 35 fracción III, 53, 54 fracción II, 57, 67 y 68 de la **"LAASSP"**, y los correlativos de su Reglamento, en términos del Oficio de Notificación de Adjudicación número 09 53 84 61 1CFG/2025/**7676**, de fecha 19 de agosto de 2025, suscrito por la Titular de la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos, documento que se integra en el **Anexo 3 (tres)** del presente contrato.

Mediante oficio número 09 53 84 61 1CFG/2025/**7695** de fecha 20 de agosto de 2025, la Titular de la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos, solicitó a la División de Contratos la elaboración del presente instrumento jurídico, remitiendo las documentales para su elaboración; siendo responsabilidad del Área Contratante, Área Requirente, Área Técnica y del Administrador del Contrato; los aspectos técnicos, presupuestales y demás cuestiones relacionadas con la contratación, incluido el contenido de los anexos, documento que se agrega en el **Anexo 3 (tres)** del presente contrato.

I.5 **"EL INSTITUTO"** cuenta con recursos suficientes y con autorización para ejercerlos en el cumplimiento de sus obligaciones derivadas del presente contrato, como se desprende del Dictamen de Disponibilidad Presupuestal Previo con cuenta número 51311014 con folio número 0000254635-2025, de fecha 11 de agosto de 2025, emitido por la Titular de la División de Control y Seguimiento al Presupuesto de Operación en Ámbito Central, mismo que se agrega al presente contrato en el **Anexo 1 (uno)**.

I.6 Cuenta con el Registro Federal de Contribuyentes **N° IMS421231I45.**

I.7 Tiene establecido su domicilio en Calle Durango número 291, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, en la Ciudad de México, mismo que señala para los fines y efectos legales del presente contrato.

II. **"EL PROVEEDOR"**, declara que:

II.1 Es una persona **MORAL** legalmente constituida según consta en la Escritura Pública número 16,515 de fecha 22 de marzo de 2007, pasada ante la fe del Licenciado Felipe Ignacio Vázquez Aldana Sauza, Titular de la Notaría Pública número 9 de la Municipalidad de

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

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

Mediante Escritura Pública número 16,970 de fecha 03 de julio de 2007, otorgada ante la fe del Licenciado Felipe Ignacio Vázquez Aldana Suza, Titular de la Notaría Pública número 9 de la Municipalidad de Tlaquepaque, Jalisco, e inscrita en el Registro Público de la Propiedad y de Comercio de la misma Entidad, con el folio mercantil electrónico número 37737*1, denominada **OPERBES, S.A. DE C.V.**

II.2 Los **C.C. Luis Alberto de la Garza Aguirre y Luis Rene Lalieu Reygadas,** en su carácter de **representantes legales**, cuenta con facultades suficientes para suscribir el presente contrato y obligar a su representada en los términos, lo cual acredita mediante la Escritura Pública número 31,724 de fecha 22 de agosto de 2024, pasada ante la fe del Licenciado Manuel Enrique Oliveros Lara, Titular de la Notaría Pública número 100 de la Ciudad de México, e inscrita en el Registro Público de Comercio de Guadalajara, Jalisco, con el folio mercantil electrónico número 37737, mismos que bajo protesta de decir verdad manifiestan que no les han sido limitados ni revocados en forma alguna.

II.3 Reúne las condiciones técnicas, jurídicas y económicas, y cuenta con la organización y elementos necesarios para su cumplimiento.

II.4 Cuenta con su Registro Federal de Contribuyentes **OPE070326DNA.**

II.5 Bajo protesta de decir verdad, está al corriente en los pagos de sus obligaciones fiscales, en específico las previstas en el artículo 32-D del Código Fiscal Federal vigente, así como de sus obligaciones fiscales en materia de seguridad social, ante el Instituto del Fondo Nacional de la Vivienda para los Trabajadores (INFONAVIT) y el Instituto Mexicano del Seguro Social (IMSS); lo que acredita con las Opiniones de Cumplimiento de Obligaciones Fiscales y en materia de Seguridad Social en sentido positivo, emitidas por el SAT e IMSS, respectivamente, así como con la Constancia de Situación Fiscal en materia de Aportaciones Patronales y Entero de Descuentos, sin adeudo, emitida por el INFONAVIT, las cuales se encuentran vigentes.

Manifiesta bajo protesta de decir verdad, no encontrarse en los supuestos de los artículos 71 y 90 de la **"LAASSP"**.

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 19 de la **"LAASSP"**.

Asimismo, manifiesta que ni él ni ninguno de los socios o accionistas desempeñan un

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

Conforme a lo previsto en los artículos 87 de la **"LAASSP"** y 107 de su Reglamento, **"EL PROVEEDOR"**, en caso de auditorías, visitas o inspecciones que practique la Secretaría Anticorrupción y Buen Gobierno y el Órgano Interno de Control Específico 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.6 Señala como su domicilio para todos los efectos legales, para oír y recibir toda clase de notificaciones y documentos el teléfono: 55 4000 2100, correo electrónico: ldelagarza@bestel.com.mx y [redacted] y domicilio ubicado en Avenida Vasco de Quiroga, número 2000, Colonia Lomas de Santa Fe, Demarcación Territorial Álvaro Obregón, Código Postal 01210, Ciudad de México.

III. De "LAS PARTES":

III.1 Que es su voluntad celebrar el presente contrato y sujetarse a sus términos y condiciones, por lo que de común acuerdo se obligan de conformidad con las siguientes:

CLÁUSULAS

PRIMERA. OBJETO DEL CONTRATO.

"EL PROVEEDOR" acepta y se obliga a proporcionar a **"EL INSTITUTO"** la prestación de los **"Servicios Administrados de Seguridad Informática (SASI) 2025", (Partida 1)**, en los términos y condiciones establecidos en este contrato y sus anexos que forman parte integrante del mismo.

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

Anexo 1 (uno) "Dictamen de Disponibilidad Presupuestal Previo"

Anexo 2 (dos) "Anexo Técnico, y Términos y Condiciones"

Anexo 3 (tres) "Propuesta Técnica y Económica, de **"EL PROVEEDOR"**, Oficio de Notificación de Adjudicación y Oficio número 09 53 84 61 1CFE/2025/**007598**"

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: CORREO ELECTRÓNICO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

Anexo 4 (cuatro) "Documento de designación de Administrador del presente Contrato"

SEGUNDA. MONTO DEL CONTRATO.

"EL INSTITUTO" pagará a **"EL PROVEEDOR"** como contraprestación por los servicios objeto de este contrato, la cantidad mínima de **$100,700,011.98 (CIEN MILLONES SETECIENTOS MIL ONCE PESOS 98/100 M.N.),** más impuestos que asciende a **$16,112,001.92 (DIECISEIS MILLONES CIENTO DOCE MIL UN PESOS 92/100 M.N.),** que hace un total de **$116,812,013.90 (CIENTO DIECISEIS MILLONES OCHOCIENTOS DOCE MIL TRECE PESOS 90/100 M.N.).**

Asimismo, el monto máximo de **$150,776,053.92 (CIENTO CINCUENTA MILLONES SETECIENTOS SETENTA Y SEIS MIL CINCUENTA Y TRES PESOS 92/100 M.N.),** más impuestos que asciende a **$24,124,168.63 (VEINTICUATRO MILLONES CIENTO VEINTICUATRO MIL CIENTO SESENTA Y OCHO PESOS 63/100 M.N.)**, que hace un total de **$174,900,222.55 (CIENTO SETENTA Y CUATRO MILLONES NOVECIENTOS MIL DOSCIENTOS VEINTIDOS PESOS 55/100 M.N.),** de conformidad con los precios unitarios que se indican en el **Anexo 3 (tres)** del presente contrato.

Los precios unitarios son considerados fijos y en pesos mexicanos hasta que concluya la relación contractual que se formaliza, incluyendo todos los conceptos y costos involucrados en la prestación de los **"Servicios Administrados de Seguridad Informática (SASI) 2025", (Partida 1)**, por lo que **"EL PROVEEDOR"** no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.

TERCERA. ANTICIPO.

Para el presente contrato **"EL INSTITUTO"** no otorgará anticipo a **"EL PROVEEDOR"**.

CUARTA. FORMA Y LUGAR DE PAGO.

"EL INSTITUTO" efectuará el pago unitario mensual conforme a las entregas programadas a **"EL PROVEEDOR"** una vez prestados los servicios, de conformidad con lo dispuesto en los artículos 73 de la **"LAASSP"** y 93 de su Reglamento, conforme a lo establecido en el numeral **13.** de los Términos y Condiciones que se agregan al presente contrato en el **Anexo 2 (dos)**.

Los pagos se realizarán en pesos mexicanos, en los plazos normados por la Dirección de Finanzas, de acuerdo al "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos" sin que éstos rebasen los 17 (diecisiete) días hábiles contados a partir del envío y verificación del Comprobante Fiscal Digital por Internet (CFDI), respectivo, siempre y cuando se cuente con la suficiencia presupuestal, así como con la documentación comprobatoria que acredite la prestación del servicio conforme lo señalado en los Términos y Condiciones que se agregan en el **Anexo 2 (dos)** del presente contrato, y conforme a los numerales cuarto y sexto del capítulo quinto, intitulado, de los Lineamientos para promover la agilización de pago a los

proveedores contenidos en el "Acuerdo por el que se emiten diversos lineamientos en materia de adquisiciones, arrendamientos y servicios y de obras públicas y servicios relacionados con las mismas", concordante con los artículos 65 y 66 del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.

El CFDI deberá presentarse ante la División de Trámite de Erogaciones de la Coordinación de Contabilidad y Trámite de Erogaciones en Órganos Normativos, la Oficina de Control de Trámite de Erogaciones en los Órganos de Operación Administrativa Desconcentrada (OOAD), la Oficina de Trámite de Erogaciones de la Unidad Médica de Alta Especialidad (UMAE), según corresponda, para proceder a su glosa, revisión y, en su caso, aprobación. En caso de aplicar, dicho CFDI deberá contener el nombre, cargo y firma de autorización del Administrador del presente Contrato, de quien suscribió la orden de compra o servicio, o de quien autorizó la contratación por montos inferiores a $2,000.00 (antes de IVA). Asimismo, en dicho CFDI se deberán indicar: número de alta en SAI o número de identificación de pedido-recepción en PREI-Millenium (cuando sea aplicable), número de proveedor, número de contrato, y la indicación de que **"EL PROVEEDOR"** cuenta con opiniones positivas y vigentes en materia de aportaciones de seguridad social ante "**EL INSTITUTO**" e INFONAVIT así como de obligaciones fiscales ante el SAT.

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

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

Para los casos en que no se formalice el presente contrato, el fallo o notificación de la adjudicación será el documento con el cual procederá el pago respectivo de los servicios proporcionados, únicamente para el periodo comprendido entre el fallo y la fecha en que debió formalizarse el presente contrato.

Para efectos de lo anterior, la División de Contratos deberá informar al administrador del presente contrato o Área Consolidadora, en su caso, en un plazo no mayor a 24 (veinticuatro) horas posteriores al vencimiento del plazo para formalización del instrumento legal, de la falta de formalización del mismo, a efecto de que se realicen las gestiones que correspondan para no recibir los servicios materia del presente contrato.

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

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

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

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

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

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

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

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 **"LAASSP"**, **"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.

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

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

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

El administrador del presente contrato llevará a cabo la valoración de la procedencia del pago por concepto de gastos no recuperables conforme a lo previsto en los artículos 101 y 102 del Reglamento de la **"LAASSP"**, en relación con los artículos 51, 67, 78 y 80, segundo párrafo de la **"LAASSP"**, previa solicitud por escrito a **"EL PROVEEDOR"**, acompañada de los documentos siguientes:

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

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

• La solicitud la realizará al administrador del presente contrato para la determinación de la procedencia del pago y, en su caso, elaborar el finiquito y remitirlo para el pago respectivo a la Coordinación de Contabilidad y Trámite de Erogaciones, dependiente de la Dirección de Finanzas, o ante la Jefatura de Servicios de Finanzas o de la Unidad Médica de Alta Especialidad (UMAE) o ante los Órganos de Operación Administrativa Desconcentrada (OOAD), según corresponda.

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

El pago de los servicios quedará condicionado proporcionalmente al pago que **"EL PROVEEDOR"** deba efectuar por conceptos de penas convencionales y/o deducciones. En ambos casos, **"EL INSTITUTO"** realizará las retenciones correspondientes sobre el CFDI que se presente para pago. En el entendido de que en el supuesto de que sea rescindido el presente contrato, no procederá el cobro de dichas penalizaciones, ni la contabilización de las mismas para

hacer efectiva la garantía de cumplimiento, de conformidad con lo establecido por el artículo 95 del Reglamento de la **"LAASSP"**.

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

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

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

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

El cómputo del plazo para realizar el pago se contabilizará a partir del día hábil siguiente de la aceptación del CFDI o factura electrónica, y ésta reúna los requisitos fiscales que establece la legislación en la materia, el desglose de los servicios prestados, los precios unitarios, se verifique su autenticidad, no existan aclaraciones al importe y vaya acompañada con la documentación soporte de la prestación de los servicios facturados.

De conformidad con el artículo 90, del Reglamento de la **"LAASSP"**, en caso de que el CFDI o factura electrónica entregado presente errores, el Administrador del presente contrato o a quien éste designe por escrito, dentro de los 3 (tres) días hábiles siguientes de su recepción, indicará a **"EL PROVEEDOR"** las deficiencias que deberá corregir; por lo que, el procedimiento de pago reiniciará en el momento en que **"EL PROVEEDOR"** presente el CFDI y/o documentos soporte corregidos y sean aceptados.

El tiempo que **"EL PROVEEDOR"** utilice para la corrección del CFDI y/o documentación soporte entregada, no se computará para efectos de pago, de acuerdo con lo establecido en el artículo 73 de la **"LAASSP"**.

El CFDI o factura electrónica se deberá presentar desglosando el impuesto cuando aplique.

"EL PROVEEDOR" manifiesta su conformidad que, hasta en tanto no se cumpla con la verificación, supervisión y aceptación de la prestación de los servicios, no se tendrán como recibidos o aceptados por el Administrador del presente contrato.

Para efectos de trámite de pago, **"EL PROVEEDOR"** deberá ser titular de una cuenta bancaria, en la que se efectuará la transferencia electrónica de pago, respecto de la cual deberá proporcionar toda la información y documentación que le sea requerida por **"EL INSTITUTO",** para efectos del pago.

"EL PROVEEDOR" deberá presentar la información y documentación **"EL INSTITUTO"** le solicite para el trámite de pago, atendiendo a las disposiciones legales e internas de **"EL INSTITUTO"**.

El pago de la prestación de los servicios recibidos, quedará condicionado al pago que **"EL PROVEEDOR"** deba efectuar por concepto de penas convencionales y, en su caso, deductivas.

Para el caso que se presenten pagos en exceso, se estará a lo dispuesto por el artículo 73, párrafo tercero, de la **"LAASSP"**.

QUINTA. LUGAR, PLAZOS Y CONDICIONES DE LA PRESTACIÓN DE LOS SERVICIOS.

La prestación de los servicios, se realizará conforme a los plazos, condiciones y entregables establecidos por **"EL INSTITUTO"** en el Anexo Técnico y en los Términos y Condiciones integrados en el **Anexo 2 (dos)** de este instrumento jurídico, apegándose a las condiciones, alcances y características detalladas en la solicitud de cotización y oficio de notificación de adjudicación, este último se agrega en el **Anexo 3 (tres)** del presente contrato.

Los servicios serán prestados en los domicilios señalados en el Anexo Técnico y en los Términos y Condiciones integrados en el **Anexo 2 (dos)** de este instrumento jurídico y fechas establecidas en los mismos.

En los casos que derivado de la verificación se detecten defectos o discrepancias en la prestación del servicio o incumplimiento en las especificaciones técnicas, **"EL PROVEEDOR"** contará con el plazo establecido en el Anexo Técnico y en los Términos y Condiciones integrados el **Anexo 2 (dos)** de este instrumento jurídico, para reposición de los servicios por motivos de fallas de calidad o cumplimiento de especificaciones originalmente convenida, sin que las sustituciones impliquen su modificación. Lo anterior, en términos del artículo 66, fracción XVII de la **"LAASSP"**.

LUGAR DE LA PRESTACIÓN DEL SERVICIO.- El **"EL PROVEEDOR"** debe prestar el servicio en las instalaciones de **"EL INSTITUTO"** ubicadas en Avenida Paseo de la Reforma número 476, Anexo de Telecomunicaciones Planta Alta, Colonia Juárez, Demarcación Territorial Cuauhtémoc, C.P. 06600, Ciudad de México.

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

PLAZO DE LA PRESTACIÓN DEL SERVICIO.- El plazo para la prestación del servicio será a partir del día hábil siguiente a la notificación de la adjudicación y hasta el 31 de diciembre de 2025, conforme a lo señalado en el Anexo Técnico y los Términos y Condiciones que se integran en el **Anexo 2 (dos)** 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 al Anexo Técnico, a los Términos y Condiciones que se integran al presente instrumento jurídico en el **Anexo 2 (dos)**, así como a lo ofrecido en sus propuestas técnica y económica que se agregan como **Anexo 3 (tres)**.

Asimismo, **"LAS PARTES"** se obligan a cumplir con lo señalado en el artículo 72 de la **"LAASSP"**.

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.

SEXTA. VIGENCIA

"LAS PARTES" convienen en que la vigencia del presente contrato será del a partir del día hábil siguiente a la notificación de la adjudicación, es decir del 20 de agosto de 2025 y hasta el 31 de diciembre de 2025.

En términos de lo señalado en el artículo 66 último párrafo de la **"LAASSP"**, el presente contrato se podrá extinguir por el cumplimiento de obligaciones.

SÉPTIMA. MODIFICACIONES DEL CONTRATO.

"LAS PARTES" están de acuerdo que **"EL INSTITUTO"** por razones fundadas y explícitas podrá ampliar el monto o la cantidad de los servicios, de conformidad con el artículo 74 de la **"LAASSP"**, siempre y cuando las modificaciones no rebasen en su conjunto el 20% (veinte por ciento) de los establecidos originalmente, el precio unitario sea igual al originalmente pactado y el presente contrato esté vigente. La modificación se formalizará mediante la celebración de un Convenio Modificatorio.

De conformidad con el artículo 68, último párrafo de la **"LAASSP"**, **"EL INSTITUTO"** con la aceptación de **"EL PROVEEDOR"** podrá realizar modificaciones al presente contrato hasta en un 20% (veinte por ciento) de la cantidad o presupuesto máximo de alguna partida originalmente pactada, utilizando para su pago el presupuesto de otra u otras partidas previstas en el propio contrato, siempre que no resulte un incremento en el monto máximo del presente instrumento jurídico, sin perjuicio de lo dispuesto en el artículo 74 de la **"LAASSP"**.

"EL INSTITUTO", podrá ampliar la vigencia del presente instrumento, siempre y cuando, no implique incremento del monto contratado o de la cantidad del servicio, siendo necesario que se obtenga el previo consentimiento de **"EL PROVEEDOR"**.

De presentarse caso fortuito o fuerza mayor, o por causas atribuibles a **"EL INSTITUTO"**, se podrá modificar el plazo del presente instrumento jurídico, debiendo acreditar dichos supuestos con las constancias respectivas. La modificación del plazo por caso fortuito o fuerza mayor podrá ser solicitada por cualquiera de **"LAS PARTES".**

En los supuestos previstos en los dos párrafos anteriores, no procederá la aplicación de penas convencionales por atraso.

Cualquier modificación al presente contrato deberá formalizarse por escrito, y deberá suscribirse por el servidor público de **"EL INSTITUTO"** que lo haya hecho, o quien lo sustituya o esté facultado para ello, para lo cual **"EL PROVEEDOR"** realizará el ajuste respectivo de la garantía de cumplimiento, en términos del artículo 91, último párrafo del Reglamento de la LAASSP, salvo que por disposición legal se encuentre exceptuado de presentar garantía de cumplimiento.

"EL INSTITUTO" se abstendrá de hacer modificaciones que se refieran a precios, anticipos, pagos progresivos, especificaciones y, en general, cualquier cambio que implique otorgar condiciones más ventajosas a **"EL PROVEEDOR"** comparadas con las establecidas originalmente.

OCTAVA. GARANTÍA DE LOS SERVICIOS.

Para la prestación de los servicios materia del presente contrato, no se requiere que **"EL PROVEEDOR"** presente una garantía por la calidad de los servicios contratados.

NOVENA. GARANTÍA DE CUMPLIMIENTO DEL CONTRATO.

Conforme a los artículos 69, fracción II y 70, fracción II de la **"LAASSP";** 85, fracción III, y 103 de su Reglamento **"EL PROVEEDOR"** se obliga a constituir una garantía **divisible** y en este caso se hará efectiva en proporción al incumplimiento de la obligación principal, mediante fianza expedida por compañía afianzadora mexicana autorizada por la Comisión Nacional de Seguros y de Fianzas, a favor de **"EL INSTITUTO",** por un importe equivalente al **10% (DIEZ POR CIENTO)** del monto máximo del presente contrato, sin incluir impuestos.

Dicha fianza deberá ser entregada a **"EL INSTITUTO"**, a más tardar dentro de los 10 días naturales posteriores a la firma del presente contrato.

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

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

EJECUCIÓN DE LA GARANTÍA DE CUMPLIMIENTO DE ESTE CONTRATO.- "EL INSTITUTO" llevará a cabo la ejecución de la garantía de cumplimiento del presente 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 presente contrato, **"EL PROVEEDOR"** no entregue en el plazo pactado el endoso o la nueva garantía, que ampare el porcentaje establecido para garantizar el cumplimiento del presente instrumento, de conformidad con la presente Cláusula.

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

En caso de que **"EL PROVEEDOR"** incumpla con la entrega de la garantía en el plazo establecido, **"EL INSTITUTO"** podrá rescindir el presente contrato y dará vista al Órgano Interno de Control Específico en **"EL INSTITUTO"** para que proceda en el ámbito de sus facultades.

La garantía de cumplimiento no será considerada como una limitante de responsabilidad de **"EL PROVEEDOR"**, derivada de sus obligaciones y garantías estipuladas en el presente instrumento jurídico, y no impedirá que **"EL INSTITUTO"** reclame la indemnización por cualquier incumplimiento que pueda exceder el valor de la garantía de cumplimiento.

En caso de incremento al monto del presente instrumento jurídico o modificación al plazo, **"EL PROVEEDOR"** se obliga a entregar a **"EL INSTITUTO",** dentro de los 10 (diez) días naturales posteriores a la formalización del mismo, de conformidad con el último párrafo del artículo 91, del Reglamento de la **"LAASSP"**, los documentos modificatorios o endosos correspondientes,

debiendo contener en el documento la estipulación de que se otorga de manera conjunta, solidaria e inseparable de la garantía otorgada inicialmente.

Una vez cumplidas las obligaciones a satisfacción, el servidor público facultado por **"EL INSTITUTO"** procederá inmediatamente a extender la constancia de cumplimiento de las obligaciones contractuales y dará inicio a los trámites para la cancelación de la garantía cumplimiento del presente contrato, lo que comunicará a **"EL PROVEEDOR".**

DÉCIMA. OBLIGACIONES DE "EL PROVEEDOR".

"EL PROVEEDOR", se obliga a:

- **a)** Prestar los servicios en las fechas o plazos y lugares establecidos conforme a lo pactado en el presente contrato y anexos respectivos.
- **b)** Cumplir con las especificaciones técnicas, de calidad y demás condiciones establecidas en el presente contrato y sus respectivos anexos.
- **c)** Asumir la responsabilidad de cualquier daño que llegue a ocasionar a **"EL INSTITUTO"** o a terceros con motivo de la ejecución y cumplimiento del presente contrato.
- **d)** Proporcionar la información que le sea requerida por la Secretaría Anticorrupción y Buen Gobierno y el Órgano Interno de Control Específico en **"EL INSTITUTO"**, de conformidad con el artículo 107 del Reglamento de la **"LAASSP"**.
- **e)** Entregar bimestralmente, las constancias de cumplimiento de la inscripción y pago de cuotas al Instituto Mexicano del Seguro Social del personal que utilice para la prestación de los servicios, en caso de aplicar.
- **f)** No podrá transferir los derechos y obligaciones que se deriven del presente contrato en favor de cualquier otra persona, con excepción de los derechos de cobro, en cuyo caso deberá contar con el consentimiento de **"EL INSTITUTO"**.
  Se exceptúa de lo anterior, en el caso de fusión, escisión o transformación de sociedades, siempre que la nueva sociedad que resulte cuente con la solvencia técnica, jurídica y económica exigidas al adjudicarse el presente contrato, cumpla con lo dispuesto en el Reglamento de la **"LAASSP"** y no se encuentre en los supuestos de impedimento previstos en la **"LAASSP"**. En ambos casos se debe contar con la autorización previa.
- **g)** Se obliga a que durante la vigencia del presente contrato se mantendrá al corriente de sus obligaciones fiscales, lo anterior, conforme a lo señalado en el artículo 66, fracción XXII de la **"LAASSP"**.
- **h)** Se obliga a integrarse al Registro de Proveedores para la Integridad ante el Instituto Mexicano del Seguro Social (REPIIMSS), en un plazo no mayor a 30 (treinta) días naturales posteriores a la formalización del presente contrato. La no integración al REPIIMSS en el plazo establecido, deberá considerarse como un incumplimiento contractual, con las consecuencias que establece la normatividad aplicable.
- **i)** Así, como a lo señalado en el Anexo Técnico y Términos y Condiciones que se integran en el **Anexo 2 (dos)** del presente contrato.

DÉCIMA PRIMERA. OBLIGACIONES DE "EL INSTITUTO".

"EL INSTITUTO", se obliga a:

a) Otorgar las facilidades necesarias, a efecto de que **"EL PROVEEDOR"** lleve a cabo en los términos convenidos la prestación de los servicios objeto del presente contrato.
b) Realizar el pago correspondiente en tiempo y forma.
c) Extender a **"EL PROVEEDOR"**, por conducto del servidor público facultado, la constancia de cumplimiento de obligaciones contractuales inmediatamente que se cumplan éstas a satisfacción expresa de dicho servidor público para que se dé trámite a la cancelación de la garantía de cumplimiento del presente contrato.
d) Así como a lo señalado en el Anexo Técnico y Términos y Condiciones que se integran en el **Anexo 2 (dos)** del presente contrato.

DÉCIMA SEGUNDA. ADMINISTRACIÓN, VERIFICACIÓN, SUPERVISIÓN Y ACEPTACIÓN DE LOS SERVICIOS.

"EL INSTITUTO" designa como Administrador del presente contrato al **C. Javier Cortés López,** con R.F.C. [redacted]**, Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información,** en el documento que se agrega al presente contrato en el **Anexo 4 (cuatro)**, quien será responsable de administrar y verificará el cumplimiento de los derechos y obligaciones establecidos en este instrumento, quien podrá ser sustituido en cualquier momento en su cargo o funciones sin que por ello sea necesario celebrar un convenio modificatorio.

Cuando **"EL INSTITUTO"** requiera efectuar el cambio o sustitución del ADMINISTRADOR DEL PRESENTE CONTRATO, o del Representante Común de éstos, sea por la ausencia temporal o definitiva del originalmente designado, o bien, por así convenir a las necesidades institucionales, bastará la nueva designación que de éste realice al Área Requirente, misma que surtirá plenos efectos a partir de la fecha en que ésta sea realizada, y que será dada a conocer a **"EL PROVEEDOR"** por el Área Requirente, o bien, por los Titulares de Órganos de Operación Administrativa Desconcentrada y de las Unidades Médicas de Alta Especialidad donde se encuentre adscrito, según corresponda. La designación que efectúe el Área Requirente en términos del presente párrafo deberá ceñirse a lo dispuesto en los numerales 4.17 y 5.3.15 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social y demás disposiciones aplicables. En ningún caso el cambio o sustitución del ADMINISTRADOR, o del Representante Común de éstos, requerirá o dará origen a la celebración de convenio modificatorio.

Los servicios se tendrán por recibidos previa revisión del administrador del presente contrato, la cual consistirá en la verificación del cumplimiento de las especificaciones establecidas y en su caso en los anexos respectivos, así como las contenidas en la propuesta técnica.

"EL INSTITUTO", a través del administrador del presente contrato, rechazará los servicios, que no cumplan las especificaciones establecidas en este contrato y en sus Anexos, obligándose **"EL PROVEEDOR"** en este supuesto a realizarlos nuevamente bajo su responsabilidad y sin costo

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: RFC, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

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

adicional para **"EL INSTITUTO",** sin perjuicio de la aplicación de las penas convencionales o deducciones al cobro correspondientes.

"EL INSTITUTO", a través del administrador del presente contrato, podrá aceptar los servicios que incumplan de manera parcial o deficiente las especificaciones establecidas en este contrato y en los anexos respectivos, sin perjuicio de la aplicación de las deducciones al pago que procedan, y reposición del servicio, cuando la naturaleza propia de éstos lo permita.

DÉCIMA TERCERA. DEDUCCIONES.

"EL INSTITUTO" aplicará deducciones al pago por el incumplimiento parcial o deficiente, en que incurra **"EL PROVEEDOR"** conforme a lo estipulado en las cláusulas del presente contrato y sus anexos respectivos, las cuales se calcularán**,** conforme al concepto (descripción del nivel de servicio), nivel de servicio, unidad de medida y porcentajes señalados en el numeral **10.** de los en los Términos y Condiciones que se integran en el **Anexo 2 (dos)** del presente contrato. Las cantidades a deducir se aplicarán en el CFDI o factura electrónica que **"EL PROVEEDOR"** presente para su cobro, en el pago que se encuentre en trámite o bien en el siguiente pago.

De no existir pagos pendientes, se requerirá a **"EL PROVEEDOR"** que realice el pago de la deductiva, en términos de la legislación aplicable.

Las deducciones económicas se aplicarán sobre la cantidad indicada sin incluir impuestos.

"EL INSTITUTO", a través del 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.

El cálculo de las deducciones correspondientes las realizará el administrador del presente contrato de **"EL INSTITUTO"**, cuyá notificación se realizará por escrito o vía correo electrónico.

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

DÉCIMA CUARTA. PENAS CONVENCIONALES.

En caso que **"EL PROVEEDOR"** incurra en atraso en el cumplimiento conforme a lo pactado para la prestación de los servicios objeto del presente contrato, conforme a lo establecido en el **Anexo 2 (dos)** parte integral del presente contrato, **"EL INSTITUTO"** por conducto del administrador del contrato aplicará la pena convencional del **1% (uno por ciento)** por cada día hábil de atraso en el inicio de la prestación del servicio, conforme a la descripción del servicio y fecha de entrega, señalados en el numeral **10.** de los Términos y Condiciones que se integran en el **Anexo 2 (dos)** del presente contrato.

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

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 Administrador determinará el cálculo de la pena convencional, cuya notificación se realizará por escrito o vía correo electrónico.

El pago de los servicios quedará condicionado, proporcionalmente, al pago que **"EL PROVEEDOR"** deba efectuar por concepto de penas convencionales por atraso; en el supuesto que el presente contrato sea rescindido en términos de lo previsto en la **CLÁUSULA VIGÉSIMA CUARTA DE RESCISIÓN**, no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento del presente contrato.

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

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

El importe de la pena convencional, no podrá exceder el equivalente al monto total de la garantía de cumplimiento del presente contrato, y en el caso de no haberse requerido esta garantía, no deberá exceder del 20% (veinte por ciento) del monto total del presente contrato.

Cuando **"EL PROVEEDOR"** quede exceptuado de la presentación de la garantía de cumplimiento, en los supuestos previsto en la **"LAASSP"**, el monto máximo de las penas convencionales por atraso que se puede aplicar, será del 20% (veinte por ciento) del monto de los servicios prestados fuera de la fecha convenida, de conformidad con lo establecido en el tercer párrafo del artículo 96 del Reglamento de la **"LAASSP"**.

DÉCIMA QUINTA. LICENCIAS, AUTORIZACIONES Y PERMISOS.

En caso de aplicar, los servicios, que de acuerdo al objeto del presente contrato se adquieran o contraten, deberán cumplir con las Normas Oficiales Mexicanas y con las Normas Mexicanas, según proceda, y a falta de éstas, con las Normas Internacionales, de conformidad con lo dispuesto en la Ley de Infraestructura de la Calidad; en su caso, con las normas de referencia o especificaciones técnicas y cumplir con las características y especificaciones requeridas en el Anexo Técnico y los Términos y Condiciones, que se agregan al presente contrato en el **Anexo 2 (dos)**.

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

DÉCIMA SEXTA. PÓLIZA DE RESPONSABILIDAD CIVIL.

Para la prestación de los servicios materia del presente contrato, no se requiere que **"EL PROVEEDOR"** contrate una póliza de seguro por responsabilidad civil.

DÉCIMA SÉPTIMA. TRANSPORTE.

"EL PROVEEDOR" se obliga bajo su costa y riesgo, a transportar los bienes e insumos necesarios para la prestación del servicio, desde su lugar de origen, hasta las instalaciones señaladas en el Anexo Técnico y en los Términos y Condiciones, que se agregan en el **Anexo 2 (dos)** del presente contrato, en caso de aplicar.

DÉCIMA OCTAVA. IMPUESTOS Y DERECHOS.

Los impuestos, derechos y gastos que procedan con motivo de la prestación de los servicios, objeto del presente contrato, serán pagados por **"EL PROVEEDOR"**, mismos que no serán repercutidos a **"EL INSTITUTO"**.

"EL INSTITUTO" sólo cubrirá, cuando aplique, lo correspondiente al Impuesto al Valor Agregado (IVA), en los términos de la normatividad aplicable y de conformidad con las disposiciones fiscales vigentes.

DÉCIMA NOVENA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES.

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

VIGÉSIMA. DERECHOS DE AUTOR, PATENTES Y/O MARCAS.

"EL PROVEEDOR" se obliga para con **"EL INSTITUTO"**, a responder por los daños y/o perjuicios que pudiera causar a **"EL INSTITUTO"** y/o a terceros, si con motivo de la prestación del servicio se violan derechos de autor, de patentes y/o marcas u otro derecho 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 66, fracción XX de la **"LAASSP"**.

Asimismo, en caso de aplicar, **"EL PROVEEDOR"** deberá observar lo establecido en el Anexo aplicable a los Derechos de autor, patentes y/o marcas del presente Contrato.

VIGÉSIMA PRIMERA. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES.

"LAS PARTES" acuerdan que la información que se intercambie de conformidad con las disposiciones del presente instrumento, se tratarán de manera confidencial, siendo de uso exclusivo para la consecución del objeto del presente contrato y no podrá difundirse a terceros de conformidad con lo establecido en la Ley General de Transparencia y Acceso a la Información Pública y Ley General de Protección de Datos Personales en posesión de Sujetos Obligados y demás legislación aplicable.

Para el tratamiento de los datos personales que **"LAS PARTES"** recaben con motivo de la celebración del presente contrato, deberá de realizarse con base en lo previsto en los Avisos de Privacidad respectivos.

Por tal motivo, **"EL PROVEEDOR"** asume cualquier responsabilidad que se derive del incumplimiento de su parte, o de sus empleados, a las obligaciones de confidencialidad descritas en el presente contrato.

Asimismo, en caso de aplicar, **"EL PROVEEDOR"** deberá observar lo establecido en el Anexo aplicable a la Confidencialidad de la información del presente Contrato.

VIGÉSIMA SEGUNDA. SUSPENSIÓN TEMPORAL DE LA PRESTACIÓN DE LOS SERVICIOS.

Con fundamento en el artículo 80 de la **"LAASSP"** y 102, fracción II, de su Reglamento, **"EL INSTITUTO"** en el supuesto de caso fortuito o de fuerza mayor o por causas que le resulten imputables, podrá suspender la prestación de los servicios, de manera temporal, quedando obligado a pagar a **"EL PROVEEDOR"**, aquellos servicios que hubiesen sido efectivamente prestados, así como, al pago de gastos no recuperables previa solicitud y acreditamiento.

Una vez que hayan desaparecido las causas que motivaron la suspensión, el presente contrato podrá continuar produciendo todos sus efectos legales, si **"EL INSTITUTO"** así lo determina; y en caso que subsistan los supuestos que dieron origen a la suspensión, se podrá iniciar la terminación anticipada del presente contrato, conforme lo dispuesto en la cláusula siguiente.

VIGÉSIMA TERCERA. TERMINACIÓN ANTICIPADA DEL CONTRATO.

"EL INSTITUTO" cuando concurran razones de interés general, de común acuerdo, o bien, cuando por causas justificadas se extinga la necesidad de proporcionar los servicios originalmente contratados 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 contrato, con motivo de la resolución de una inconformidad o intervención de oficio, emitida por la Secretaría Anticorrupción y Buen Gobierno, podrá dar por terminado anticipadamente el presente contrato sin responsabilidad alguna para **"EL INSTITUTO"**, ello con independencia de lo establecido en la cláusula que antecede.

Cuando **"EL INSTITUTO"** determine dar por terminado anticipadamente el presente contrato, lo notificará a **"EL PROVEEDOR"** hasta con 30 (treinta) días naturales anteriores al hecho, y se sustentará mediante dictamen que se precise las razones o las causas justificadas que dieron origen a la misma, de conformidad con lo señalado en el artículo 78 de la **"LAASSP"**, una vez notificada la terminación anticipada, se extinguirá el presente contrato, lo que dará lugar a formalizar el finiquito entre **"LAS PARTES"**.

"EL INSTITUTO" pagará a **"EL PROVEEDOR"** la parte proporcional de los servicios proporcionados, así como los gastos no recuperables en que haya incurrido, previa solicitud por escrito, siempre que estos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente contrato, limitándose según corresponda a los conceptos establecidos en la fracción I, del artículo 102 del Reglamento de la **"LAASSP"**.

VIGÉSIMA CUARTA. RESCISIÓN.

"EL INSTITUTO" podrá iniciar en cualquier momento el procedimiento de rescisión, cuando **"EL PROVEEDOR"** incurra en alguna de las siguientes causales:

a) Contravenir los términos pactados para la prestación de los servicios, establecidos en el presente contrato.
b) Transferir en todo o en parte las obligaciones que deriven del presente contrato a un tercero ajeno a la relación contractual.
c) Ceder los derechos de cobro derivados del presente contrato, sin contar con la conformidad previa y por escrito de **"EL INSTITUTO"**.
d) Suspender total o parcialmente y sin causa justificada la prestación de los servicios del presente contrato.
e) No realizar la prestación de los servicios en tiempo y forma conforme a lo establecido en el presente contrato y sus respectivos anexos.
f) No proporcionar a los Órganos de Fiscalización, la información que le sea requerida con motivo de las auditorías, visitas e inspecciones que realicen.
g) Ser declarado en concurso mercantil, o por cualquier otra causa distinta o análoga que afecte su patrimonio.
h) En caso de que compruebe la falsedad de alguna manifestación, información o documentación proporcionada para efecto del presente contrato;

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

i) No presentar bimestralmente, las constancias de la inscripción y pago de cuotas al Instituto Mexicano del Seguro Social del personal que utilice para la prestación de los servicios; en caso de aplicar.
j) No entregar dentro de los 10 (diez) días naturales posteriores a la fecha de firma del presente contrato, la garantía de cumplimiento del mismo.
k) En caso de que la suma de las penas convencionales o las deducciones al pago, igualan el monto total de la garantía de cumplimiento del presente contrato y/o alcanzan el 20% (veinte por ciento) del monto total de este contrato cuando no se haya requerido la garantía de cumplimiento;
l) Divulgar, transferir o utilizar la información que conozca en el desarrollo del cumplimiento del objeto del presente contrato, sin contar con la autorización de **"EL INSTITUTO"** en los términos de lo dispuesto en la CLÁUSULA VIGÉSIMA PRIMERA CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES del presente instrumento jurídico;
m) Impedir el desempeño normal de labores de **"EL INSTITUTO";**
n) Incumplir cualquier obligación distinta de las anteriores y derivadas del presente contrato.

Para el caso de optar por la rescisión del presente contrato, **"EL INSTITUTO"** de conformidad con lo establecido en el artículo 77 de la **"LAASSP"**, comunicará a **"EL PROVEEDOR"** el incumplimiento en que haya incurrido, para que en un término de 5 (cinco) días hábiles contados a partir de la notificación, exponga lo que a su derecho convenga y aporte, en su caso, las pruebas que estime pertinentes.

Transcurrido dicho término, **"EL INSTITUTO"** en un plazo de 10 (diez) días hábiles, tomando en consideración los argumentos y pruebas que hubiere hecho valer **"EL PROVEEDOR"**, determinará de manera fundada y motivada dar o no por rescindido el presente contrato, y comunicará a **"EL PROVEEDOR"**, en términos de lo dispuesto en el artículo 77 de la **"LAASSP"**, dicha determinación dentro del citado plazo.

Cuando se rescinda el presente contrato, se extinguirán los derechos los derechos y obligaciones del mismo, y se formulará el finiquito correspondiente, a efecto de hacer constar los pagos que deba efectuar **"EL INSTITUTO"** por concepto de los servicios proporcionados hasta el momento de la rescisión, o los que resulten a cargo de **"EL PROVEEDOR".**

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

Si previamente a la determinación de dar por rescindido el presente contrato se realiza la prestación de los servicios, el procedimiento iniciado quedará sin efecto, previa aceptación y verificación de **"EL INSTITUTO"** de que continúa vigente la necesidad de la prestación de los servicios, aplicando, en su caso, las penas convencionales correspondientes.

"EL INSTITUTO" podrá determinar no dar por rescindido el presente contrato, cuando durante el procedimiento advierta que la rescisión del mismo 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 presente contrato resultarían más inconvenientes.

De no rescindirse el presente contrato, **"EL INSTITUTO"** establecerá con **"EL PROVEEDOR"**, otro plazo, que le permita subsanar el incumplimiento que hubiere motivado el inicio del procedimiento, aplicando las sanciones correspondientes. El convenio modificatorio que al efecto se celebre deberá atender a las condiciones previstas por los dos últimos párrafos del artículo 74 de la **"LAASSP"**.

No obstante, de que se hubiere firmado el convenio modificatorio a que se refiere el párrafo anterior, si se presenta de nueva cuenta el incumplimiento, **"EL INSTITUTO"** quedará expresamente facultada para optar por exigir el cumplimiento del presente contrato, o rescindirlo, aplicando las sanciones que procedan.

Si se llevara a cabo la rescisión del presente contrato, y en el caso de que a **"EL PROVEEDOR"** se le hubieran entregado pagos progresivos, éste deberá de reintegrarlos más los intereses correspondientes, conforme a lo indicado en el artículo 73, párrafo cuarto, de la **"LAASSP"**.

Los intereses se calcularán sobre el monto de los pagos progresivos efectuados 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"**.

VIGÉSIMA QUINTA. RELACIÓN Y EXCLUSIÓN LABORAL

"EL PROVEEDOR" reconoce y acepta ser el único patrón de todos y cada uno de los trabajadores que intervienen en la prestación del servicio, deslindando de toda responsabilidad a **"EL INSTITUTO"** respecto de cualquier reclamo que en su caso puedan efectuar sus trabajadores, sea de índole laboral, fiscal o de seguridad social y en ningún caso se le podrá considerar patrón sustituto, patrón solidario, beneficiario o intermediario.

"EL PROVEEDOR" asume en forma total y exclusiva las obligaciones propias de patrón respecto de cualquier relación laboral, que el mismo contraiga con el personal que labore bajo sus órdenes o intervenga o contrate para la atención de los asuntos encomendados por **"EL INSTITUTO"**, así como en la ejecución de los servicios.

Para cualquier caso no previsto, **"EL PROVEEDOR"** exime expresamente a **"EL INSTITUTO"** de cualquier responsabilidad laboral, civil o penal o de cualquier otra especie que en su caso pudiera llegar a generarse, relacionado con el presente contrato.

Para el caso que, con posterioridad a la conclusión del presente contrato, **"EL INSTITUTO"** reciba una demanda laboral por parte de trabajadores de **"EL PROVEEDOR"**, en la que se

demande la solidaridad y/o sustitución patronal a **"EL INSTITUTO"**, **"EL PROVEEDOR"** queda obligado a dar cumplimiento a lo establecido en la presente cláusula.

VIGÉSIMA SEXTA. DISCREPANCIAS.

La convocatoria a la licitación pública, la invitación a cuando menos tres personas, o la solicitud de cotización, según corresponda del procedimiento de contratación citado en la declaración **I.4** del presente instrumento jurídico, este contrato y sus anexos son los instrumentos que vinculan a **"LAS PARTES"** en sus derechos y obligaciones.

"LAS PARTES" convienen que, en caso de discrepancia entre la convocatoria a la licitación pública, la invitación a cuando menos tres personas, o la solicitud de cotización, según corresponda del procedimiento de contratación del cual deriva el presente instrumento jurídico, y el modelo de contrato, prevalecerá lo establecido en la convocatoria, invitación o solicitud respectiva, de conformidad con el artículo 81, fracción IV, del Reglamento de la **"LAASSP"**.

VIGÉSIMA SÉPTIMA. CONCILIACIÓN.

"LAS PARTES" acuerdan que para el caso de que se presenten desavenencias derivadas de la ejecución y cumplimiento del presente contrato podrán someterse al procedimiento de conciliación establecido en los artículos 109, 111 y 112 de la **"LAASSP"**, y 126 al 136 de su Reglamento.

VIGÉSIMA OCTAVA. DOMICILIOS Y NOTIFICACIONES.

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

Sin perjuicio de lo anterior, **"EL PROVEEDOR"** acepta explícitamente que las notificaciones que le sean remitidas al correo electrónico manifestado en el apartado de Declaraciones surtirán plenos efectos, en términos de lo dispuesto en el artículo 35, fracción II, de la Ley Federal de Procedimiento Administrativo.

VIGÉSIMA NOVENA. LEGISLACIÓN APLICABLE.

"LAS PARTES" se obligan a sujetarse estrictamente para la prestación de los servicios objeto del presente contrato a todas y cada una de las cláusulas que lo integran, sus anexos que forman parte integral del mismo, a la **"LAASSP"**, su Reglamento; Código Civil Federal; Ley Federal de Procedimiento Administrativo, Código Federal de Procedimientos Civiles; Ley Federal de Presupuesto y Responsabilidad Hacendaria y su Reglamento.

TRIGÉSIMA. JURISDICCIÓN.

"LAS PARTES" convienen que, para la interpretación y cumplimiento de este contrato, así como para lo no previsto en el mismo, se someterán a la jurisdicción y competencia de los Tribunales Federales con sede en la Ciudad de México, renunciando expresamente al fuero que pudiera corresponderles en razón de su domicilio actual o futuro.

FIRMANTES O SUSCRIPCIÓN.

Por lo anterior expuesto, **"EL INSTITUTO"** y **"EL PROVEEDOR"**, manifiestan estar conformes y enterados de las consecuencias, valor y alcance legal de todas y cada una de las estipulaciones que el presente instrumento jurídico contiene, por lo que lo ratifican y firman electrónicamente en las fechas especificadas en cada firma electrónica.

POR:
"EL INSTITUTO"

NOMBRE	CARGO	R.F.C.
C. ELIA SANDRA VARAS GALEANA	Titular de la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos y Apoderada Legal	[redacted]
C. JAVIER CORTÉS LÓPEZ	Titular Coordinación de Telecomunicaciones y Seguridad de la Información	

POR:
"EL PROVEEDOR"

NOMBRE	R.F.C.
OPERBES, S.A. DE C.V.	OPE070326DNA

RRSR/HRJ/JMHN/CLGR

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: RFC, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: RFC, NO. DE SERIE, CADENA, CERTIFICADO Y FIRMA, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

Contrato: 050GYR019N15725-001-00

Cadena original:

[redacted]

Firmante: JAVIER CORTES LOPEZ
RFC[redacted]

Número de Serie:[redacted]
Fecha de Firma: 05/09/2025 15:10

Certificado:

[redacted]

Firma:

[redacted]

Firmante: ELIA SANDRA VARAS GALEANA
RFC:[redacted]

Número de Serie[redacted]
Fecha de Firma: 05/09/2025 15:26

Certificado:

[redacted]

Firma:

[redacted]

Firmante: OPERBES SA DE CV
RFC: OPE070326DNA

Número de Serie:[redacted]
Fecha de Firma: 05/09/2025 19:36

Certificado:

[redacted]

Firma:

Contrato: 050GYR019N15725-001-00

H3SUKI62HFTNiF40gTtYRMKgjIvlzCTeRXhAJx/Rk6jH5bwqeeCGqsolQXqnc1hjwrbEsH192FpgTzRxrX4LJWWDTZCbGWGXpRW7WMg35kd91FLt7XsqpyxqRfKCMtubQq1K9mXIWxrn1RydUVccoDZQ/0nG/mi4
CBM0qVVYuaficUenof/kvlXwV1JGE6+BSUNC1I2Ozl7dnJc+ajnio2KvB0bV8jVywne7GnqS5jaQSQbpXg20VWKZ/qhFWW4bJNK0fgnOcIrNfUljxV/8Q7wn/cNiZBbBdJhew4gwcnJPFBtwr0DsJJ1GFqI+ls7y
8dt3whH/BpJRpPMYbzKUOA==

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** **050GYR019N15725-001-00**

ANEXO 1 (UNO)

"DICTAMEN DE DISPONIBILIDAD PRESUPUESTAL PREVIO"

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

INSTITUTO MEXICANO DEL SEGURO SOCIAL

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

FOLIO: 0000254635-2025

[ ] Dictamen de Inversión
[X] Dictamen de Gasto

Dependencia Solicitante: 09 Distrito Federal Nivel Central
099001 Oficinas Centrales
500000 Direccion Innovacion Y Desarro

Concepto: OF. 1499 RECIBIDO 08/08/2025 - "SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMATICA (SASI) 2025", (PARTIDA 1), PARA EL EJERCICIO 2025.

Fecha Elaboración: 11/08/2025

Total Comprometido (en pesos): $ 175,855,926.30
Cuenta: 51311014 Serv Int Infraestructura Compu Unidad de Información: 099001 Centro de Costos: 500000
COG 3190401

COMPROMETIDO MENSUAL (en miles de pesos)

ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
0.0	0.0	0.0	0.0	0.0	0.0	0.0	116,416.6	14,859.8	14,859.8	29,719.7	0.0

DISPONIBLE (en miles de pesos)

0.0	0.0	0.0	0.0	0.0	0.0	0.0	131,896.8	625.0	811.8	0.0	0.0

El presente documento de existencia de respaldo presupuestario se emite en términos de lo señalado en los artículos 8, 144 y 148 del Reglamento Interior del Instituto Mexicano del Seguro Social (IMSS), y el numeral 7.5.9.4 de la Norma Presupuestaria del IMSS, es responsabilidad del área solicitante el destino y aplicación de los recursos. También se informa que este documento únicamente tendrá validez para el ejercicio fiscal en curso, y que con base en la revisión que se efectuó en el Sistema FINAT, 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

Laura Victoria López Pinajero
Titular Div de Ctrl y Seguimiento al Ppto de Oper en Ámbito Central

DIA	MES	AÑO

DICTAMINADO DEFINITIVO

DICTAMEN DEFINITIVO

INSTITUTO MEXICANO DEL SEGURO SOCIAL
COORDINACIÓN TÉCNICA DE GESTIÓN PRESUPUESTARIA
DIVISIÓN DE CONTROL Y SEGUIMIENTO AL PRESUPUESTO DE OPERACIÓN EN EL ÁMBITO CENTRAL
VERIFICACIÓN PRESUPUESTAL

CONTRATO No.

IMPORTE DEFINITIVO (EN PESOS) : $ .00

ANEXOS
DIVISIÓN DE CONTRATOS

Clave: 6170-009-001

SIN TEXTO

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 050GYR019N15725-001-00

ANEXO 2 (DOS)

"ANEXO TÉCNICO, Y TÉRMINOS Y CONDICIONES"

ANEXOS
DIVISIÓN DE CONTRATOS

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

SIN TEXTO

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
Ver 0.1	31/05/2024	Actualización del Documento	Lic. Cynthia Osmara Verdín Villegas
Ver 0.2	31/05/2024	Revisión del Documento	Ing. Abraham Gutiérrez Castillo
Ver 1.0	31/05/2024	Aprobación del Documento	Lic. Florencio Fernando González Velázquez
Ver 1.1	01/09/2024	Ajustes/Revisión del documento	Ing. Abraham Gutiérrez Castillo
Ver 2.0	01/09/2024	Aprobación del documento	Ing. Javier Cortes López

Contenido

a) Descripción amplia y detallada de los bienes a adquirir o arrendar o servicios solicitados. 3
I. Características y especificaciones. 3
i. Objetivo 3
ii. Alcance 4
iii. Requerimientos técnicos 5
iv. Especificaciones técnicas 5
iv.1 Servicios de Seguridad – Continuidad Operativa 5
iv.1.1 Servicios de Firewall 5
iv.1.2 Servicios de Prevención de Intrusos (IPS) 7
iv.1.3 Servicios de Protección contra Denegación de Servicio (DDoS) 8
iv.1.4 Servicios de Redes Privadas Virtuales (VPN) 10
iv.1.5 Servicios de Filtrado de Contenido Web 12
iv.1.6 Servicios de Filtrado de Contenido de Correo (Antispam) 13
iv.1.7 Servicios de Firewall Especializado en Servicios Web (WAF) 15
iv.1.8 Servicios de Firewall especializado en Base de Datos (DBF) 16
iv.1.9 Servicios de Gestión Unificada de Amenazas (UTM) 18
iv.1.10 Servicio de Correlación de Eventos 20
iv.1.11 Servicio de Protección de Amenazas Persistentes Avanzadas (APT) 21
iv.2 Servicios de Seguridad – Verificación y Calidad 23
iv.2.1 Servicios de Borrado Seguro de Información 23
iv.2.2 Servicio de Gestión de Dominios 25
iv.2.3 Servicio de Certificados Digitales SSL 26
iv.2.4 Servicios de Ciberinteligencia (Ciberseguridad) 26
iv.2.5 Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos Móviles. 29
iv.2.6 Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA). 30
iv.2.7 Servicio de Antivirus 31

ANEXOS
DIVISIÓN DE CONTRATOS

iv.2.8 Servicios de Prevención de Pérdida de Información 33
iv.2.9 Servicios de Sistema de Gestión de Seguridad de la Información (SGSI) 34
iv.2.10 Servicios Continuidad de Gestión del Cambio en Seguridad de la Información 38
iv.2.11 Servicios del Centro de Operaciones de Seguridad (SOC) 39
iv.2.12 Servicios de Análisis de Vulnerabilidades Dinámico 42
iv.2.13 Servicios de Análisis de Vulnerabilidades Estático 43
iv.2.14 Servicios de Pruebas de Penetración 43
iv.2.15 Servicios de Análisis Forense 45
v. Perfil del Proveedor 46
vi. Condiciones técnicas de aceptación de entregable 49
vii. Cronograma de actividades 61
viii. Niveles de servicio acordados que deberán cumplirse 62
ix. Requerimientos de arquitectura tecnológica 62
x. Restricciones e interfaces con otros elementos 62
b) Pruebas requeridas, método de evaluación y el resultado mínimo que debe obtenerse al ejecutar las pruebas. 62
c) Modificaciones de la especificación técnica de algún bien que no se encuentre regulado por el compendio nacional de insumos para la salud. 62
d) Modificaciones de la especificación técnica de un bien respecto de las estipuladas en el ejercicio anterior. 63
e) Firmas de elaboración, revisión y aprobación 65
f) Relación de Anexos 65

ANEXOS
DIVISIÓN DE CONTRATOS

a) Descripción amplia y detallada de los bienes a adquirir o arrendar o servicios solicitados.

La clave del Clasificador Único de las Contrataciones Públicas (CUCOP) de los bienes a adquirir o arrendar o servicios solicitados se identifica en la siguiente tabla:

Clave CUCOP	31900004
Descripción	Servicios a centros de datos (hospedaje, electricidad, video vigilancia, monitoreo, aire acondicionado, servidores y otros
Unidad de Medida	Servicio
Partida Específica (COG)	31904 "Servicios Integrales de Infraestructura de Computo"
Objetivo del contrato	Servicios Administrados de Seguridad Informática

I. Características y especificaciones.

i. Objetivo

Para garantizar la continuidad operativa y la seguridad de la información del IMSS, se habilitarán dos partidas que operarán de forma independiente (contratos independientes).

Debido a la naturaleza diferenciada de los servicios contemplados en cada partida, no resulta adecuado que un mismo proveedor atienda ambas. Esta separación es necesaria para asegurar la imparcialidad en la prestación, supervisión y evaluación de los servicios, evitando que un proveedor pueda intervenir simultáneamente en funciones que deben mantenerse independientes entre sí. Permitir que un solo proveedor participe en ambas partidas implicaría un posible conflicto de interés, al asumir un rol operativo y de validación al mismo tiempo, lo cual lo colocaría en una posición de juez y parte. Por lo anterior, se debe asegurar que cada partida sea adjudicada a un proveedor distinto, como se ha hecho en experiencias contractuales previas.

Estas partidas incluirán:

1. **Continuidad en Operación:** Esto incluirá la continuidad de procesos operativos y atención de cambios, gestión de riesgos, supervisión continuad de servicios de seguridad para asegurar una continuidad operativa eficiente.
2. **Servicios de Infraestructura:** Abarcará la operación, soporte y mantenimiento de la infraestructura existente en los centros de datos, así como en las localidades donde el Instituto tenga activos que apoyen a la operación. Además, proporcionará atención a los servicios y aplicaciones del instituto. Se asegurará que la infraestructura sea confiable, segura y capaz de satisfacer las necesidades operativas del IMSS.
3. **Protección Integral de Servidores, Aplicaciones y Bases de Datos:** Se brindará un servicio completo de protección para los servidores, aplicaciones y bases de datos del IMSS. Esto incluirá medidas preventivas y reactivas para garantizar la integridad y disponibilidad de los datos críticos.

Se dará continuidad operativa a las soluciones avanzadas de seguridad para hacer frente a las amenazas actuales y emergentes.

4. **Servicios de Seguridad de la Información Especializados:** Este servicio se centrará en aspectos específicos relacionados con las tecnologías de la información, comunicaciones y seguridad de la información.

Objetivos específicos

- Salvaguardar y proteger la información institucional.
- Garantizar la continuidad operativa, de negocio y la seguridad de la información durante la vigencia del presente contrato.
- Reforzar la seguridad de la información contra posibles amenazas, reduciendo el riesgo de incidentes de seguridad mediante la aplicación de tecnología de vanguardia para la supervisión, detección, aseguramiento, contención y respuesta ante posibles ataques a la infraestructura de cómputo, sistemas y aplicaciones del IMSS.
- Contar con servicios de infraestructura regulados por niveles de servicio que incluyan la implementación de componentes necesarios en los centros de datos y servicios del IMSS, así como la gestión integral de la infraestructura para satisfacer las necesidades de conectividad, comunicación, protección, control y filtrado de la institución, asegurando que la plataforma tecnológica opere en óptimas condiciones.
- Disponer de servicios de protección de manera unificada e integrada, abarcando la prevención de pérdida de información, protección de sistemas físicos o virtuales, protección del correo electrónico interno y externo, herramientas de colaboración y trazabilidad, así como el filtrado e inspección del acceso a internet e intranet mediante una solución integral que permita la gestión consolidada de funcionalidades y servicios, con el fin de mantener, asegurar y fortalecer el esquema de seguridad del IMSS.
- Contar con servicios de seguridad de la información que complementen de manera consistente y robusta el esquema de seguridad institucional, incluyendo el control, aseguramiento, diagnóstico, pruebas, metodologías, acceso a cuentas privilegiadas, bases de datos, aplicaciones, correlación y trazabilidad de eventos, investigación forense y otros servicios especializados en seguridad y tecnologías de la información.

ii. Alcance

El alcance del SASI 2025 abarca los siguientes aspectos:

1. Un esquema de servicios para la gestión y monitoreo de la infraestructura física y lógica de seguridad necesaria para la supervisión de los centros de datos. Este esquema incluye la operación, soporte y mantenimiento de la infraestructura existente, así como la posibilidad de su sustitución para mantener una plataforma tecnológicamente moderna y uniforme, garantizando la continuidad operativa, empresarial y la seguridad de la información del IMSS.
2. Un esquema de servicios de protección que ofrece una solución integral, cubriendo la protección de los servicios de colaboración internos, el correo electrónico externo y la navegación web. Este esquema detecta y protege contra amenazas avanzadas, previene la fuga de información y se gestiona de manera consolidada.
3. Un esquema de servicios de seguridad que complementa el esquema de protección. Incluye servicios orientados a firewalls, sistemas de prevención de intrusiones (IPS), filtrado de contenido, protección contra ataques de denegación de servicio distribuido (DDoS), antispam, firewall de aplicaciones web (WAF), protección de bases de datos (DBF), redes privadas virtuales (VPN). Además, se ofrece análisis de vulnerabilidades, análisis forense, pruebas de penetración, borrado seguro de información, aseguramiento de aplicaciones, ciberinteligencia, servicios de protección para redes inalámbricas y

dispositivos móviles, gestión y control de acceso para usuarios privilegiados, correlación de eventos, protección contra amenazas persistentes avanzadas (APT), gestión de procesos de seguridad y servicios especializados en seguridad de la información. Este esquema proporciona una cobertura completa de seguridad.

iii. Requerimientos técnicos

Los requerimientos técnicos se encuentran integrados en el Anexo Técnico junto con sus Apéndices A y B.

1) Funcionales

Los requerimientos técnicos se encuentran integrados en el Anexo Técnico junto con sus Apéndices A y B.

2) No funcionales

Los requerimientos no funcionales se encuentran integrados en los Términos y Condiciones.

iv. Especificaciones técnicas

Partida 1.

iv.1 Servicios de Seguridad – Continuidad Operativa

iv.1.1 Servicios de Firewall

Descripción del servicio: El instituto requiere garantizar la continuidad operativa del servicio que proporciona seguridad y protección, incluyendo el control de acceso, filtrado y bloqueo contra ataques dirigidos a las aplicaciones, así como la inspección de paquetes a nivel de aplicación para identificar patrones de tráfico anómalo. Por consiguiente, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas:

• Garantizar la continuidad operativa de los activos de infraestructura actualmente en uso por el Instituto, mediante el suministro de soporte técnico, licenciamiento y otros recursos necesarios. Esto asegurará cumplir con los niveles de servicio establecidos en el apéndice B.

• Desarrollar en colaboración con el Instituto la estrategia de habilitación para mantener la continuidad operativa de los activos de infraestructura actuales o los que sean necesarios según las necesidades operativas del Instituto.

• Realizar las acciones requeridas para la instalación del equipo en los Centros de Datos correspondientes o en cualquier otra ubicación designada por el Instituto.

• Coordinar con el personal del Instituto, a través del administrador del contrato o del modelo de gobierno designado, las ventanas de mantenimiento necesarias para garantizar el correcto funcionamiento del servicio. No se podrán realizar cambios en los componentes de hardware o software sin la autorización correspondiente.

ANEXOS
DIVISIÓN DE CONTRATOS

• Continuar con la integración de cada activo de infraestructura en su consola de administración centralizada, ya sea en modo stand alone o para la administración de todos los dispositivos, y asegurar que los registros de actividad de cada activo estén integrados en la solución de correlación de eventos del proyecto o en otra designada por el Instituto para este propósito.

• Garantizar que los activos de infraestructura cuenten con actualizaciones tecnológicas estables y validadas del sistema operativo, aplicaciones (firmware) y otros componentes necesarios.

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

•Mantener el acceso a los servicios alojados en la capa de servidores de los centros de datos (DMZ), gestionando según el esquema de seguridad establecido y respetando la segmentación entre las diferentes zonas de seguridad.

•Prevenir la explotación de vulnerabilidades y el ingreso de tráfico malicioso a las redes del Instituto.

•Atender todos los requerimientos de cambio, incidencias/fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos para tal fin.

•Monitorear todos los eventos registrados en la solución y emitir alertas sobre incidentes generados por los activos de infraestructura del servicio.

•Notificar actividades sospechosas relacionadas con la violación de políticas y aquellas identificadas a través de funcionalidades habilitadas en la solución.

•Informar sobre fallas relacionadas con el hardware de los activos de infraestructura provistos a través del servicio.

•Gestionar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como realizar todas las renovaciones requeridas durante la vigencia de los servicios.

•Realizar evaluaciones operativas de los servicios (herramientas de software y activos de infraestructura) y análisis de vulnerabilidades cada seis meses desde el inicio de operaciones y hasta seis meses antes del término de los servicios. Estas evaluaciones deben identificar mejoras en el rendimiento de los activos, gestión de configuraciones y nuevas funcionalidades operativas derivadas de actualizaciones de hardware y/o software.

•Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos, como componentes de comunicación entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

•Proporcionar al Instituto cuentas de acceso a las consolas de administración correspondientes al servicio, así como herramientas en software para acceder a las mismas, garantizando que sean de solo lectura y que los atributos de consulta se definan según las mesas correspondientes.

•Suministrar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre casos de soporte, documentación técnica, pólizas de mantenimiento, licenciamiento adquirido y otros datos relevantes para la toma de decisiones sobre el uso del servicio.

•Implementar un servicio de auditoría de reglas de acceso en los dispositivos firewall para el análisis y depuración de estas, mejorando así el control de acceso y la seguridad. Esta solución se ubicará en las instalaciones del centro de datos primario y no generará costos adicionales para el Instituto.

• Garantizar el cumplimiento de las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.2 Servicios de Prevención de Intrusos (IPS)

Descripción del servicio: El Instituto requiere garantizar la continuidad operativa del servicio que proporciona protección perimetral basada en firmas y que identifica vulnerabilidades. Este servicio tiene como objetivo contener intentos de acceso no autorizado a los recursos o servicios publicados en Internet o Intranet que podrían afectar la operación de la organización, detectar accesos no autorizados y prevenir fugas de información. Por lo tanto, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas:

• Garantizar la continuidad operativa de los activos de infraestructura actuales del Instituto, proporcionando el soporte técnico, licenciamiento u otros recursos necesarios para asegurar esta continuidad operativa, así como cumplir con los niveles de servicio requeridos, según lo establecido en el Apéndice B.

• Coordinar con el personal del Instituto, a través del administrador del contrato o del modelo de gobierno designado, las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio. No se podrán realizar cambios en los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por el Instituto.

• Continuar integrando cada activo de infraestructura en su consola de administración centralizada, ya sea en modo stand-alone para la administración de todos los dispositivos, y asegurar que los registros de actividad de cada activo estén integrados en la solución de correlación de eventos del proyecto o en otra designada por el Instituto.

• Garantizar que los activos de infraestructura cuenten con actualizaciones tecnológicas estables y validadas del sistema operativo, aplicaciones (firmware) y otros componentes necesarios.

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

• Prevenir la explotación de vulnerabilidades y el ingreso de tráfico malicioso a las redes del Instituto.

• Atender todos los requerimientos de cambio, incidentes/fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos.

• Monitorear todos los eventos registrados en la solución y emitir alertas sobre incidentes generados por los activos de infraestructura que componen el servicio.
•Notificar cualquier actividad sospechosa relacionada con la violación de políticas, así como aquellas identificadas mediante las funcionalidades habilitadas en la solución.

• Informar sobre fallas relacionadas con el hardware de los activos de infraestructura proporcionados a través del servicio.

ANEXOS
DIVISIÓN DE CONTRATOS

• Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como llevar a cabo todas las renovaciones necesarias durante la vigencia de los servicios.

• Realizar evaluaciones operativas de los servicios y análisis de vulnerabilidades cada seis meses, desde el inicio de operaciones y hasta seis meses antes del término de estos, para identificar mejoras en el rendimiento de los activos, en la gestión de configuraciones y en la detección de nuevas funcionalidades operativas derivadas de actualizaciones de hardware y/o software.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en el presente Anexo Técnico, incluyendo componentes que faciliten la comunicación entre redes, el cableado eléctrico y de datos, el montaje en racks, entre otros.

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

• Suministrar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licenciamiento adquirido para cada servicio proporcionado y otros datos relevantes para la toma de decisiones sobre el uso del presente servicio.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos IPS para el análisis y depuración de estas, así como para mejorar el control de acceso y la seguridad. Esta solución se implementará en las instalaciones del centro de datos primario y no generará costos adicionales para el instituto.

• Cumplir, como mínimo, con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.3 Servicios de Protección contra Denegación de Servicio (DDoS)

Descripción del servicio: El Instituto requiere mantener la continuidad operativa del servicio que brinda protección contra los ataques de denegación de servicio distribuido, basado en firmas y altos volúmenes de conexión. Por lo tanto, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas:

• Asegurar la continuidad operativa de los activos de infraestructura actuales del Instituto, proporcionando el soporte técnico, licenciamiento u otros recursos necesarios para garantizar esta continuidad operativa, así como cumplir con los niveles de servicio requeridos para este propósito, según lo establecido en el Apéndice B.

• Dar continuidad operativa a traves de una solución híbrida con activos de infraestructura de propósito junto con una solución de nube para mantener la continuidad operativa del Instituto, conforme a lo dispuesto en el Apéndice A.

• Definir en colaboración con el Instituto la estrategia para habilitar la continuidad operativa de los activos de infraestructura actuales o los necesarios para cubrir las necesidades operativas.

• Realizar las tareas necesarias para instalar el equipo en los Centros de Datos correspondientes, o en cualquier otra ubicación solicitada por el Instituto.

• Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado, las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio. En ningún momento se podrán realizar cambios en los componentes de hardware o software que integran el servicio sin un control de cambios autorizado por el Instituto.

• Continuar integrando cada activo de infraestructura en su respectiva consola de administración centralizada, pudiendo ser en modo stand-alone para la administración de todos los dispositivos, y asegurar que la bitácora de cada activo esté integrada en la solución de correlación de eventos del proyecto o en otra designada por el Instituto.

• Garantizar que los activos de infraestructura cuenten con actualizaciones tecnológicas estables y validadas del sistema operativo, aplicación (firmware) y otros componentes necesarios.

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

• Continuar con el acceso a los servicios ubicados en la capa de servidores de los centros de datos (DMZ), gestionando 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, incidentes/fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos para dicho propósito.

• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura que componen el servicio, incluyendo:

- Notificar actividades sospechosas relacionadas con la violación de las políticas, así como las identificadas a través de las funcionalidades habilitadas en la solución.
- Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura proporcionados a través del servicio.

• Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como realizar todas las renovaciones necesarias durante la vigencia de los servicios.

• Realizar evaluaciones operativas a los servicios (herramienta de software y activos de infraestructura), así como análisis de vulnerabilidades, para identificar mejoras en el desempeño de los activos, gestión de configuraciones y detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Estas evaluaciones se llevarán a cabo cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de estos.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en este Anexo Técnico, como componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.

ANEXOS
DIVISIÓN DE CONTRATOS

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas en software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otros disponibles). Estas cuentas serán de solo lectura, y sus atributos de consulta se definirán en las mesas establecidas para este propósito.

• Facilitar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licenciamiento adquirido para cada servicio proporcionado y otros datos relevantes para la toma de decisiones sobre el uso del servicio.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos DDoS para el análisis, depuración y mejor control de acceso y seguridad. Esta solución se implementará en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.

• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.4 Servicios de Redes Privadas Virtuales (VPN)

Descripción del servicio: El Instituto requiere garantizar la continuidad operativa del servicio de interconexión a través de Internet, el cual posibilita establecer comunicaciones desde localidades remotas para la transferencia de información mediante un canal cifrado. Por lo tanto, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas:

• Garantizar la continuidad operativa de los activos de infraestructura existentes en el Instituto, así como implementar los recursos necesarios para mantener esta continuidad, incluyendo soporte técnico, licenciamiento y cualquier otro requerimiento para cumplir con los niveles de servicio establecidos en el Apéndice B.

• Definir en colaboración con el Instituto la estrategia para asegurar la continuidad operativa de los activos de infraestructura actuales y futuros, de acuerdo con las necesidades operativas.

• Realizar las tareas necesarias para la instalación del equipo en los centros de datos correspondientes, o en cualquier otra ubicación requerida por el Instituto.

• Coordinar con el personal del Instituto, mediante el administrador del contrato o el modelo de gobierno designado, las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio. No se podrán realizar cambios en los componentes de hardware o software sin la autorización correspondiente.

• Proseguir con la integración de cada activo de infraestructura en su respectiva consola de administración centralizada, ya sea en modo independiente o stand alone, asegurando que la bitácora de cada activo esté integrada en la solución de correlación de eventos designada por el Instituto.

• Garantizar que los activos de infraestructura cuenten con actualizaciones tecnológicas del sistema operativo, aplicaciones (firmware) y otros componentes necesarios para su funcionamiento.

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

• Continuar proporcionando acceso a los servicios ubicados en la capa de servidores de los centros de datos (DMZ), gestionando según el esquema de seguridad establecido 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 todas las solicitudes de cambio, incidentes, fallos y solicitudes de información generadas por el Instituto, siguiendo los Niveles de Servicio establecidos para tales fines.

• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura que conforman el servicio, cumpliendo al menos con lo siguiente:

- Notificar cualquier actividad sospechosa relacionada con la violación de las políticas, así como aquellas identificadas mediante las funcionalidades habilitadas en la solución.
- Informar sobre las fallas relacionadas con el hardware de los activos de infraestructura proporcionados a través del servicio.

•Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, incluyendo todas las renovaciones requeridas durante la duración de los servicios.

• Realizar evaluaciones operativas de los servicios, herramientas de software y activos de infraestructura, así como análisis de vulnerabilidades, con el fin de identificar mejoras en el rendimiento de los activos, en la gestión de configuraciones y en la detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Estas evaluaciones se llevarán a cabo cada 6 meses, desde el inicio de la operación de los servicios hasta 6 meses antes de su finalización.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en este Anexo Técnico, incluyendo componentes que faciliten las comunicaciones entre redes, el cableado eléctrico y de datos, el montaje en racks, entre otros.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas de software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otros disponibles), las cuales serán de solo lectura. Los atributos de consulta se definirán en las mesas integradas para este propósito.

• Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licenciamiento adquirido para cada servicio proporcionado, entre otros aspectos relevantes para la toma de decisiones sobre el uso del servicio.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos VPN para el análisis y depuración de estas, así como para mejorar el control de acceso y la seguridad. Esta solución deberá implementarse en las instalaciones del centro de datos primario sin generar costos adicionales para el instituto.

• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

ANEXOS
DIVISIÓN DE CONTRATOS

iv.1.5 Servicios de Filtrado de Contenido Web

Descripción del servicio: El Instituto requiere garantizar la continuidad operativa del servicio de filtrado de contenido web, el cual permite controlar y filtrar el acceso a Internet según roles y perfiles definidos. En este sentido, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas:

• Garantizar la continuidad operativa de los activos de infraestructura actualmente en posesión del Instituto, así como la implementación de nuevos activos si fuera necesario. Esto incluye el soporte técnico, licenciamiento y cualquier otro requerimiento necesario para asegurar dicha continuidad operativa, todo de acuerdo con los niveles de servicio establecidos en el Apéndice B.

• Colaborar con el Instituto en la definición de la estrategia para habilitar la continuidad operativa de los activos de infraestructura actuales o los que se necesiten según los requisitos operativos.

• Realizar la instalación del equipo necesario en los Centros de Datos designados o en cualquier otra localidad requerida por el Instituto.

• Coordinar con el personal del Instituto, ya sea a través del administrador del contrato o el cuerpo de gobierno designado, las ventanas de mantenimiento necesarias para asegurar el correcto funcionamiento del servicio. No se podrán realizar cambios en los componentes de hardware o software que integran el servicio sin la autorización correspondiente.

• Continuar integrando cada activo de infraestructura en su respectiva consola de administración centralizada, permitiendo la administración independiente (stand-alone) de los dispositivos, y asegurando que la bitácora de cada activo se integre adecuadamente en la solución de correlación de eventos del proyecto o en otra designada por el Instituto.

• Asegurar que los activos de infraestructura estén actualizados tecnológicamente, con un sistema operativo, aplicación (firmware) u otro componente necesario, estable y validado.

• Limitar el tráfico de datos únicamente al definido por el Instituto, tanto interno como externo, entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.

• Mantener el acceso a los servicios ubicados en la capa de servidores de los centros de datos (DMZ), gestionándolos de acuerdo con el esquema de seguridad establecido y respetando la segmentación definida entre las diferentes zonas de seguridad.

• Evitar la explotación de vulnerabilidades y el ingreso de tráfico malicioso a las redes del Instituto.

• Gestionar todos los requerimientos de cambio, incidentes/fallas y solicitudes de información generadas por el Instituto, siguiendo los Niveles de Servicio establecidos para dicho propósito.

• Monitorear todos los eventos registrados en la solución y emitir alertas sobre incidentes generados por los activos de infraestructura que integran el servicio, cumpliendo al menos con:

- Notificar actividades sospechosas relacionadas con la violación de políticas y aquellas identificadas mediante las funcionalidades habilitadas en la solución.

- Notificar sobre fallos relacionados con el hardware de los activos de infraestructura proporcionados a través del servicio.

• Integrar el licenciamiento del software necesario para mantener en funcionamiento los servicios y activos de infraestructura correspondientes, así como llevar a cabo todas las renovaciones requeridas durante la duración de los servicios.

• Realizar evaluaciones operativas a los servicios (herramientas de software y activos de infraestructura), así como análisis de vulnerabilidades, con el fin de identificar mejoras en el rendimiento de los activos, en la gestión de configuraciones, y detectar nuevas funcionalidades operativas derivadas de actualizaciones en las versiones de hardware y/o software. Estas evaluaciones se ejecutarán cada 6 meses, desde el inicio de las operaciones de los servicios hasta 6 meses antes de su finalización.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en el presente Anexo Técnico, como componentes que permitan la comunicación entre redes, el cableado eléctrico y de datos, el montaje en racks, entre otros.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas de software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otras disponibles). Estas cuentas serán de solo lectura, y los atributos de consulta se definirán en las mesas integradas para este propósito.

• Facilitar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licenciamiento adquirido para cada servicio proporcionado, y otros recursos que ayuden en la toma de decisiones sobre el uso del presente servicio.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos de Filtrado de Contenido Web para realizar análisis y depuración de estas, y mejorar el control de acceso y seguridad. Esta solución se implementará en las instalaciones del centro de datos primario sin incurrir en costos adicionales para el instituto.

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

iv.1.6 Servicios de Filtrado de Contenido de Correo (Antispam)

Descripción del servicio: El Instituto busca garantizar la continuidad operativa de un servicio destinado al análisis de correos electrónicos de entrada y salida. Este servicio tiene como finalidad bloquear aquellos correos que sean identificados como spam, *malware*, *phishing*, o que contengan contenido malicioso, entre otros. Por lo tanto, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas.

•Garantizar la continuidad operativa de los activos de infraestructura existentes en el Instituto. Esto incluye el soporte técnico, licenciamiento y cualquier otro requerimiento necesario para mantener la operatividad, de acuerdo con los niveles de servicio establecidos en el Apéndice B.

• Trabajar en conjunto con el Instituto para definir la estrategia de habilitación que asegure la continuidad operativa de los activos de infraestructura actuales y futuros, según las necesidades operativas.

• Ejecutar todas las tareas necesarias para instalar el equipo en los Centros de Datos correspondientes, atendiendo las solicitudes del Instituto.

• Dar continuidad operativa a los servicio de protección para el correo electrónico entrante y saliente, así como salvaguardar la reputación de las direcciones IP utilizadas para la comunicación en Internet, mediante un mecanismo de sanitización en la nube que brinde una doble capa de verificación sobre correos anómalos o no deseados.

• Establecer, en coordinación con el personal del Instituto, las ventanas de mantenimiento necesarias para la correcta operación del servicio, asegurando que cualquier cambio en los componentes de hardware o software esté autorizado.

• Mantener la integración de cada activo de infraestructura hacia su consola de administración centralizada, garantizando la integración de la bitácora de cada activo en la solución de correlación de eventos designada por el Instituto.

•Asegurar que los activos de infraestructura cuenten con actualizaciones tecnológicas del sistema operativo, aplicaciones (firmware) u otros componentes necesarios para su correcto funcionamiento.

• Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central y otros puntos de interconexión con redes externas.

• Continuar permitiendo el acceso a servicios ubicados en la capa de servidores de los centros de datos, gestionándolos según el esquema de seguridad establecido y respetando la segmentación entre las zonas de seguridad.

• Implementar medidas proactivas para evitar la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

• Brindar atención a todos los requerimientos de cambio, incidentes, fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos.

• Supervisar todos los eventos registrados en la solución y enviar alertas sobre incidentes generados por los activos de infraestructura del servicio, incluyendo notificaciones sobre actividades sospechosas y fallas de hardware.

- 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.

• Incluir el licenciamiento del software necesario para mantener los servicios y activos de infraestructura, así como realizar renovaciones durante la vigencia del contrato.

• Realizar evaluaciones periódicas de los servicios y activos de infraestructura para identificar mejoras y detectar nuevas funcionalidades operativas, así como analizar vulnerabilidades cada 6 meses.

• Implementar integraciones de conectividad física y lógica para habilitar los servicios descritos, incluyendo componentes como cableado, montaje en racks, entre otros.

• Facilitar al Instituto cuentas de acceso a las consolas de administración del servicio y a las bases de conocimiento de las tecnologías integradas, con información relevante para la toma de decisiones.

• Implementar un servicio de auditoría de reglas de acceso en dispositivos Antispam para mejorar el control de acceso y seguridad, sin costo adicional para el Instituto.

• Asegurar el cumplimiento de las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.7 Servicios de Firewall Especializado en Servicios Web (WAF)

Descripción del servicio. El Instituto requiere garantizar la continuidad del servicio de protección, prevención y control de ataques dirigidos a los aplicativos *web* expuestos en Internet/Intranet. Por ende, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas.

• Garantizar la continuidad operativa de los activos de infraestructura existentes en el Instituto, así como la implementación de cualquier recurso adicional necesario para mantener esta continuidad, lo que incluye soporte técnico, licenciamiento y cualquier otro requisito necesario para asegurar el servicio de acuerdo con lo estipulado en el Apéndice B.

• Colaborar con el Instituto para definir la estrategia de habilitación que asegure la continuidad operativa de los activos de infraestructura actuales y aquellos que sean necesarios para satisfacer las necesidades operativas.

• Realizar las tareas requeridas para instalar el equipo en los Centros de Datos correspondientes o en cualquier otra ubicación solicitada por el Instituto.

• Coordinar con el personal del Instituto, a través del administrador del contrato o del modelo de gobierno designado, las ventanas de mantenimiento necesarias para garantizar el correcto funcionamiento del servicio, asegurando que cualquier cambio en los componentes de hardware o software esté autorizado por el Instituto.

• Continuar integrando cada activo de infraestructura en su respectiva consola de administración centralizada, ya sea de forma independiente o en modo stand alone, asegurando que la bitácora de cada activo se integre en la solución de correlación de eventos designada por el Instituto.

• Garantizar la actualización tecnológica de los activos de infraestructura, incluyendo el sistema operativo, la aplicación (firmware) u otros componentes necesarios para el servicio correspondiente.

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

• Mantener el acceso a los servicios en la capa de servidores de los centros de datos (DMZ), gestionándolos 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 en las redes del Instituto.

• Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información generados por el Instituto, cumpliendo con los Niveles de Servicio definidos para este propósito.

• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura que componen el servicio, notificando actividades sospechosas relacionadas con la violación de políticas o fallas en el hardware de los activos de infraestructura provistos a través del servicio.

- Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como realizar todas las renovaciones necesarias durante la vigencia de los servicios.

- Realizar evaluaciones operativas y análisis de vulnerabilidades de los servicios y activos de infraestructura para identificar mejoras en el desempeño, gestión de configuraciones y detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software, ejecutándose cada 6 meses desde el inicio de operaciones hasta 6 meses antes del término de estos.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en el Anexo Técnico, como componentes 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 servicio correspondiente, así como herramientas de software para acceder a las mismas, las cuales deben ser de solo lectura y cuyos atributos de consulta deben ser definidos en las mesas que se integren para este propósito.

• Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas, 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, entre otros aspectos relevantes para la toma de decisiones respecto al uso del servicio.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos WAF para analizar y depurar las mismas, mejorando el control de acceso y seguridad, con la solución implementada en las instalaciones del centro de datos primario sin costo adicional para el Instituto.

• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.8 Servicios de Firewall especializado en Base de Datos (DBF)

Descripción del servicio: El Instituto requiere mantener la operatividad continua del servicio de protección para las instancias de bases de datos en tiempo real, así como supervisar el tráfico de la base de datos para detectar ataques avanzados. Por lo tanto, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas.

•Garantizar la continuidad operativa de los activos de infraestructura del Instituto, proporcionando soporte técnico, licenciamiento y otros recursos necesarios para asegurar dicha continuidad, conforme a lo establecido en el Apéndice B.

• Definir en colaboración con el Instituto la estrategia de habilitación para mantener la continuidad operativa de los activos de infraestructura actuales o los que sean necesarios según las necesidades operativas.

• Realizar la instalación del equipo en los Centros de Datos correspondientes o en otras ubicaciones solicitadas por el Instituto.

• Acordar con el personal del Instituto, ya sea a través del administrador del contrato o el modelo de gobierno designado, las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio, y abstenerse de realizar cambios en los componentes de hardware o software sin una autorización de cambio previa.

• Continuar integrando cada activo de infraestructura en su respectiva consola de administración centralizada, ya sea en modo stand-alone para la administración de todos los dispositivos o mediante otras configuraciones requeridas, garantizando la integración de las bitácoras de cada activo en la solución de correlación de eventos definida por el Instituto.

• Garantizar la actualización tecnológica de los activos de infraestructura, incluyendo el sistema operativo, aplicación (firmware) y otros componentes necesarios.

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

• Mantener el acceso a los servicios ubicados en la capa de servidores de los centros de datos (Base de datos), gestionando según el esquema de seguridad y respetando la segmentación definida entre las zonas de servidores.

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

• Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información generados por el Instituto, cumpliendo con los Niveles de Servicio definidos.

• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura del servicio, notificando sobre actividades sospechosas relacionadas con la violación de las políticas y fallas relacionadas con el hardware de los activos de infraestructura.

- 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.

ANEXOS
DIVISIÓN DE CONTRATOS

• Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como realizar todas las renovaciones necesarias durante la vigencia de los servicios.

• Realizar evaluaciones operativas y análisis de vulnerabilidades a los servicios y activos de infraestructura cada 6 meses, desde el inicio de operaciones hasta 6 meses antes del término de estos, identificando mejoras en el desempeño, gestión de configuraciones y nuevas funcionalidades operativas.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en el Anexo Técnico, 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 servicio, así como herramientas en software que permitan acceder a las mismas, garantizando que sean de solo lectura y definiendo los atributos de consulta en las mesas correspondientes.

• Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas, donde se pueda consultar información sobre casos de soporte, documentación técnica, pólizas de mantenimiento vigentes, licenciamiento adquirido, y otras que faciliten la toma de decisiones.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos DBF para mejorar el control de acceso y seguridad, implementado en las instalaciones del centro de datos primario sin costo adicional para el Instituto.

• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.9 Servicios de Gestión Unificada de Amenazas (UTM)

Descripción del servicio: El Instituto busca asegurar la continuidad operativa del servicio de protección perimetral especializado en control de acceso, prevención de intrusos, filtrado de contenido web y VPN, con el fin de controlar el tráfico y detectar actividades anómalas. Por lo tanto, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

• Garantizar la continuidad operativa de los activos de infraestructura existentes en el Instituto. Esto incluye proporcionar soporte técnico, licenciamiento y cualquier otro requisito para garantizar esta continuidad operativa, en conformidad con lo establecido en el Apéndice B.

• Definir en colaboración con el Instituto la estrategia para habilitar la continuidad operativa de los activos de infraestructura actuales o los nuevos requeridos para satisfacer las necesidades operativas.

• Realizar todas las tareas necesarias para instalar el equipo en los Centros de Datos correspondientes, o en cualquier otra ubicación solicitada por el Instituto.

• Acordar con el personal del Instituto, a través del administrador del contrato o el modelo de gobierno designado, las ventanas de mantenimiento necesarias para garantizar el correcto funcionamiento del servicio, asegurando que cualquier cambio en los componentes de hardware o software del servicio sea autorizado mediante un control de cambios.

• Continuar integrando cada activo de infraestructura en su consola de administración centralizada respectiva, ya sea en modo independiente o en conjunto, y asegurar que el registro de cada activo esté integrado en la solución de correlación de eventos especificada por el Instituto.

• Garantizar que los activos de infraestructura estén actualizados tecnológicamente, incluyendo el sistema operativo, la aplicación (firmware) u otros componentes necesarios para el servicio correspondiente.

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

• Prevenir la explotación de vulnerabilidades y el ingreso de tráfico malicioso a las redes del Instituto.

• Atender todos los requerimientos de cambio, incidentes/fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos.

• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura que componen el servicio, notificando actividades sospechosas relacionadas con violaciones de políticas y fallas en hardware.

- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
- Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

• Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura, incluyendo todas las renovaciones requeridas durante la vigencia de los servicios.

• Realizar evaluaciones operativas y análisis de vulnerabilidades a los servicios y activos de infraestructura cada seis meses, identificando mejoras en el desempeño, la gestión de configuraciones y la detección de nuevas funcionalidades operativas.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en el Anexo Técnico, como componentes de comunicación entre redes, cableado eléctrico y de datos, y montaje en racks.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas de software para acceder a las mismas, con atributos de consulta definidos en mesas de trabajo específicas.

• Proporcionar al Instituto acceso a bases de conocimiento de las tecnologías integradas, donde se pueda consultar información sobre casos de soporte, documentación técnica, pólizas de mantenimiento y licenciamiento adquirido para cada servicio proporcionado.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos UTM para análisis, depuración y mejor control de acceso y seguridad, sin generar costo adicional para el Instituto.

ANEXOS
DIVISIÓN DE CONTRATOS

• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.10 Servicio de Correlación de Eventos

Descripción del servicio: El Instituto requiere un servicio de seguridad que gestione, analice, explote, utilice y aproveche los registros de actividad de los dispositivos de seguridad para comprender completamente lo que sucede en varios puntos de la red de manera centralizada y eliminar los falsos positivos generados. Por lo tanto, el proveedor debe cumplir con las siguientes especificaciones funcionales mínimas.

• Proveer activos de infraestructura de última generación, exclusivamente dedicados a satisfacer las necesidades del Instituto.

• Habilitar los activos de infraestructura en esquemas de Alta Disponibilidad (HA).

• Definir en colaboración con el Instituto la estrategia para habilitar los nuevos activos de infraestructura para la correlación de eventos en la arquitectura de seguridad y comunicaciones.

• Ejecutar todas las tareas necesarias para instalar el equipo en los Centros de Datos correspondientes, o en cualquier otra ubicación requerida por el Instituto.

• Coordinar con el personal del Instituto, a través del administrador del contrato o el modelo de gobierno designado, todas las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio. No se realizarán cambios a los componentes de hardware/software sin un control de cambios autorizado por el Instituto.

• Integrar cada activo de infraestructura en su respectiva consola de administración centralizada, ya sea en modo independiente (stand alone) para la administración de todos los dispositivos, asegurando que la bitácora de cada activo esté integrada en la solución de correlación de eventos del proyecto o en otra designada por el Instituto.

• Garantizar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada del sistema operativo, aplicación (firmware) u otro componente necesario.

• Permitir únicamente la correlación definida por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión vía syslog con otras redes o nubes.

• Atender los requerimientos de cambio, atención de fallas y solicitudes de información generadas por el Instituto, según los Niveles de Servicio definidos.

• Monitorear los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura del servicio, notificando actividades sospechosas relacionadas con la violación de las políticas y fallas de hardware.

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

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

• En caso de rendimiento inadecuado, presentar propuestas de mejora de los activos afectados y sustituir componentes tecnológicos por otros de igual o mejores características/funcionalidades, con autorización previa del Instituto.

• Integrar el licenciamiento del software necesario para habilitar los servicios y activos de infraestructura correspondientes, así como realizar renovaciones durante la vigencia de los servicios.

• Realizar evaluaciones operativas cada 6 meses para identificar mejoras en el desempeño de los activos, gestión de configuraciones y detección de nuevas funcionalidades, derivadas de actualizaciones en versiones de hardware y/o software.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio y herramientas en software de solo lectura, cuyos atributos de consulta se definirán en mesas específicas.

• Proporcionar al Instituto cuentas de acceso a bases de conocimiento de las tecnologías integradas para la solución, incluyendo información sobre casos de soporte, documentación técnica, pólizas de mantenimiento y licenciamiento adquirido.

• Incluir un servicio de auditoría de reglas de acceso en los dispositivos del Correlacionador de Eventos para análisis, depuración y mejor control de acceso y seguridad, implementado en las instalaciones del centro de datos primario sin costo adicional para el Instituto.

• Cumplir, como mínimo, con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.11 Servicio de Protección de Amenazas Persistentes Avanzadas (APT)

Descripción del servicio: El Instituto busca un servicio que le brinde la capacidad de protegerse contra amenazas avanzadas que puedan estar activas dentro de la organización y que hayan eludido los controles de seguridad existentes. En este sentido, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

• Proveer activos de infraestructura de última generación, dedicados exclusivamente a las necesidades del Instituto.

• Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA).

• Definir en colaboración con el Instituto la estrategia para habilitar los nuevos activos de infraestructura para la detección de Amenazas Persistentes Avanzadas en la arquitectura de seguridad y comunicaciones.

• Ejecutar las tareas necesarias para la instalación del equipo en los Centros de Datos correspondientes, o en cualquier otra ubicación solicitada por el Instituto.

ANEXOS
DIVISIÓN DE CONTRATOS

• Coordinar con el personal del Instituto, a través del administrador del contrato o el cuerpo de gobierno designado, todas las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio, sin realizar cambios a los componentes de hardware/software sin autorización.

• Integrar cada activo de infraestructura en su respectiva consola de administración centralizada, asegurando que la bitácora de cada activo quede integrada en la solución de correlación de eventos designada por el Instituto.

• Garantizar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada del sistema operativo, aplicación (firmware) u otro componente necesario.

• Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes o nubes, previniendo la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

• Atender los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información generadas por el Instituto, apegado a los Niveles de Servicio definidos.

• Monitorear los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura del servicio, notificando actividades sospechosas relacionadas con la violación de las políticas y fallas de hardware.

- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
- Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

• En caso de rendimiento inadecuado, presentar propuestas de mejora de los activos afectados y sustituir componentes tecnológicos por otros de igual o mejores características/funcionalidades, con autorización previa del Instituto.

• Integrar el licenciamiento del software necesario para habilitar los servicios y activos de infraestructura correspondientes, así como realizar renovaciones durante la vigencia de los servicios.

• Realizar evaluaciones operativas cada 6 meses para identificar mejoras en el desempeño de los activos, gestión de configuraciones y detección de nuevas funcionalidades, derivadas de actualizaciones en versiones de hardware y/o software.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio y herramientas en software de solo lectura, cuyos atributos de consulta se definirán en mesas específicas.

• Proporcionar al Instituto cuentas de acceso a bases de conocimiento de las tecnologías integradas para la solución, incluyendo información sobre casos de soporte, documentación técnica, pólizas de mantenimiento y licenciamiento adquirido.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos del servicio de Amenazas Persistentes Avanzadas para análisis, depuración y mejor control de acceso y seguridad, implementado en las instalaciones del centro de datos primario sin costo adicional para el Instituto.

• Cumplir, como mínimo, con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.2 Servicios de Seguridad – Verificación y Calidad

El Instituto requiere la verificación de controles de seguridad durante la vigencia del contrato, los cuales coadyuvaran a identificar, clasificar, atender y priorizar la confidencialidad, integridad y disponibilidad de la información contenida en equipos de usuarios final, así como en aplicativos institucionales.

El proyecto tiene por objeto dar continuidad al modelo operativo actualmente en ejecución, por lo que las actividades contempladas en el servicio de verificación corresponden a los procesos de:

- Revisión de cumplimiento de políticas de seguridad institucional,
- Validación periódica de configuraciones técnicas en los activos monitoreados,
- Verificación de integridad operativa de los componentes de seguridad,
- Y seguimiento de no conformidades en los reportes generados.

El servicio está orientado a la verificación continua de los procesos y servicios de seguridad informática actualmente en operación, sin incorporación de nuevos alcances, productos o componentes tecnológicos.

En ese sentido, a continuación, se describen las características técnicas de los servicios que integran estos procesos de verificación y calidad:

iv.2.1 Servicios de Borrado Seguro de Información

Descripción del servicio: Se busca mantener la solución de borrado seguro de información para una variedad de dispositivos, incluyendo computadoras personales, laptops, servidores, unidades de almacenamiento fijas y removibles, así como cualquier otro dispositivo determinado por el Instituto. El objetivo es evitar la pérdida y dispersión de información propiedad del Instituto cuando estos dispositivos sean retirados debido a razones como la conclusión de contratos, obsolescencia, fallas, bajas o reasignaciones, entre otros motivos. Para lograrlo, es necesario renovar el derecho de uso y soporte técnico de los productos de software de borrado seguro, así como actualizar el licenciamiento correspondiente. Estas actualizaciones (updates y upgrades) deben garantizar la confidencialidad de la información del Instituto, cumpliendo con la legislación vigente sobre derechos de autor.

El proveedor de servicios deberá cumplir con las siguientes especificaciones funcionales mínimas y asegurar que los servicios y entregas de información estén de conformidad con la normativa aplicable para dichas soluciones y servicios.

• Integrar todas las renovaciones 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.

• Permitir la realización de borrados completos en medios de almacenamiento dispuestos en activos de infraestructura como equipos de cómputo (de escritorio y portátiles), equipos de propósito específico (appliance), servidores físicos o virtuales, derivado de la sustitución, migraciones o retiro por finalización del contrato.

ANEXOS
DIVISIÓN DE CONTRATOS

• 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, tanto de estado sólido como mecánicos, independientemente de su tamaño.

• Destrucción local y/o remota en múltiples dispositivos de almacenamiento.

• Capacidades para desmontar RAID (SCSI) cuando sea necesario.

• Facilitación del proceso de borrado y detección de zonas bloqueadas/ocultas (DCO, HPA).

• Generación de certificados de borrado infalsificables, incluyendo el resultado del proceso de borrado, fecha, hora, detalles del equipo y del dispositivo de almacenamiento borrado, con el fin de ofrecer protección legal.

• Emisión de una firma electrónica para autenticar la integridad del reporte de sanitización emitido por el software de borrado.

• Ejecución de la solución sin importar el sistema operativo utilizado.

• Exportación del reporte generado por la solución a un medio de almacenamiento como USB o disco duro.

• El servicio de borrado seguro se proporciona a través de un proceso operativo que incluye:

- Solicitud de borrado.
- Identificación del medio a borrar.
- Definición de fecha para el borrado.
- Flujos operativos para autorización de borrado o destrucción.
- Se muestran los insumos a ser atendidos como referencia.

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

DISPOSITIVOS
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

• Es fundamental que la continuidad del servicio garantice que los usuarios tengan acceso a las consolas de administración de la solución. Esto les permitirá gestionar, administrar, supervisar y operar, con el objetivo de habilitar las funcionalidades necesarias para llevar a cabo el borrado seguro de manera descentralizada, incluso en oficinas remotas.

iv.2.2 Servicio de Gestión de Dominios

Descripción del servicio: Garantizar la continuidad operativa para el registro y gestión de dominios conforme a los requisitos establecidos por el NIC. El proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas:

El proveedor deberá realizar entre otros:

• El Registro de nombre de dominio cuya titularidad será en beneficio del Instituto Mexicano de Seguro Social, incluyendo al menos:

- Seguimiento ante las instancias certificadoras o gestoras de dominios para México.
- Coordinación con el personal designado por el Instituto para la gestión, pago y procesos administrativos del dominio acordado o solicitado
- Verificación de duplicidad o uso por terceros del nombre de dominio solicitados por el Instituto, privilegiando aquellos que están facultados para entidades de Gobierno en la Administración Pública Federal.
- Supervisión del alojamiento del dominio a traves de terceros confiables.
- Actualización de las directivas de seguridad relacionadas con la expedición de dominios:
    - Fechas de vencimiento
    - Periodos de renovación
    - Actualización de datos de contacto para recibir soporte técnico
- Mantenimiento de los dominios conforme lo plazos de vencimiento establecidos por los terceros confiables.
- Notificaciones de cambio de políticas para la publicación de nombres de dominio.
- Adecuada transferencia de dominios al cambiar de proveedor de servicios.

El proveedor de servicios deberá encargarse de la gestión y los pagos relacionados con el registro, cambio de dominio o proveedor, sin costos adicionales para el Instituto.

El proveedor deberá emitir las evidencias de actualización de dominios en forma digital, conforme cada solicitud realizada por el Instituto.

ANEXOS
DIVISIÓN DE CONTRATOS

iv.2.3 Servicio de Certificados Digitales SSL

Descripción del Servicio: Se busca garantizar la continuidad del servicio para obtener certificados SSL destinados a proteger las páginas web del Instituto durante la duración del contrato. Por lo tanto, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas:

- Encripción SSL con al menos las siguientes características:
  - Cifrado SHA 256 RSA
  - Cifrado de Curva Elíptica (ECC)
  - Dominio principal conforme la solicitud generada por el Instituto
  - Llave publica RSA de al menos 1024 bits.
  - Validación extendida y privacidad contra sitios fraudulentos (phishing)
  - Vigencia de al menos 12 meses
- Los certificados deben ser emitidos por una Autoridad Certificadora de Confianza (tercero confiable)
- No se aceptará certificados emitidos por autoridades no confiables (certificados autofirmados), o por entidades que no puedan comprobar la reputación de un tercero confiable
- El proveedor deberá realizar la validación de certificados y sus fechas de vencimientos conforme las solicitudes realizadas por el Instituto.
- El tiempo de emisión debe cumplir con los niveles de servicio establecidos para su entrega al personal del Instituto y será vía correo electrónico.
- El proveedor se encargará de la gestión de los pagos de derechos y cualquier otro cargo asociado a la obtención y mantenimiento de los certificados.
- Los certificados deben ser compatibles con las versiones vigentes de intérpretes web (navegación como Chrome, Edge, Firefox,Safari, entre otros)
- Los certificados deben ser compatibles con al menos dispositivos móviles con sistema operativos iOS, Android.

• 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).
- Certificados para código.

iv.2.4 Servicios de Ciberinteligencia (Ciberseguridad)

Descripción del servicio: El Instituto busca un servicio de inteligencia con capacidad de acción que le permita responder de manera oportuna ante amenazas o ataques informáticos detectados a través de campañas y operaciones identificadas, así como realizar investigaciones según sus necesidades. Por lo tanto, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas:

• Detección de posible venta de información confidencial del Instituto en mercado negro.

• Seguimiento de grupos hacktivistas y del cibercrimen nacionales y extranjeros que representen una amenaza para el Instituto.

• Infiltración en canales de IRC donde se organicen y difundan campañas de ataques informáticos que puedan afectar al Instituto.

• Monitoreo de foros y comunidades en redes abiertas y en la Red Onion/Tor donde se perpetren y difundan campañas de ataques informáticos que representen un riesgo para el Instituto.

• Vigilancia de noticias nacionales y extranjeras en la red abierta y en la Deep web para recopilar inteligencia táctica que permita al Instituto tomar acciones preventivas adicionales para proteger su infraestructura de posibles ataques informáticos.

• Recopilación de información a través de un cuestionario especializado para realizar el análisis de la situación global del Instituto y generar perfiles de investigación para los servicios permanentes.

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

• Análisis de la situación global del Instituto teniendo en cuenta el contexto del entorno y la identificación de exposiciones y amenazas que podrían impactarle, tanto a nivel local como global.

• Generación de perfiles de investigación con la información recabada, incluyendo perfiles virtuales a emplear y definición de fuentes asociadas a los perfiles virtuales utilizados en el monitoreo.

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

• Establecimiento de umbrales para eventos que desencadenarán alertas hacia la matriz de notificación definida en conjunto con el Instituto para los servicios de "Vigilancia Permanente de Ciberinteligencia".

• Mantenimiento de supervisión de correos/sitios de phishing y direcciones IP sospechosas proporcionadas por el Instituto para su análisis. Además, se llevará a cabo vigilancia continua en el ciberespacio las 24 horas del día, los 365 días del año, incluyendo redes sociales, Darknet y buscadores de Internet de las cosas. Se utilizarán técnicas de OSINT (Inteligencia de Fuentes Abiertas) como líneas de tiempo y mapas de conexiones, así como Virtual HUMINT para la infiltración de perfiles virtuales.

• Identificación de campañas para ataques específicos, venta de información y exposición de infraestructura vulnerable en Internet, así como relaciones entre perfiles y grupos privados de Facebook, entre otros.

• Realización de evaluaciones en los siguientes casos:

- Durante la vigilancia de Ciberinteligencia al identificar una amenaza real para el Instituto.
- Cuando se solicite análisis de sitios o correos de phishing, o direcciones IP.
- Durante análisis de grupos hacktivistas.
- Durante análisis de direcciones IP de ataques de denegación de servicio experimentados por el Instituto.

• Realizar un análisis correlacionando información recolectada con eventos específicos y emisión de dictámenes con inteligencia accionable hacia el Instituto en un plazo máximo de 24 horas después de la

ANEXOS
DIVISIÓN DE CONTRATOS

detección de eventos críticos, como ataques de denegación de servicio, defacements, fuga de información, phishing, entre otros.

- Declaración de posibles ataques de denegación de servicio por parte de grupos hacktivistas o del cibercrimen.
- Defacements.
- Fuga de información confidencial del Instituto hacia sitios públicos.
- Malware dirigido.
- Phishing detectado en parking domains.
- Indicios de amenazas o ataques informáticos sobre el Instituto.
- Existencia de campañas (conjunto de acciones para perpetrar un ataque informático) en contra del Instituto.
- Venta o publicación de información sensible del Instituto en la Darknet.
- Publicación de información confidencial de personal del Instituto como usuarios y contraseñas.
- Nuevos esquemas de fraude detectados en otros organismos del sector.

• Generación de procesos de inteligencia accionable en casos donde se haya detectado un ataque con impacto en el Instituto o en análisis a petición del Instituto sobre phishing y direcciones IP, proporcionando recomendaciones pertinentes.

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

• Análisis mensual de direcciones IP sospechosas para identificar posibles actividades de ataque, intrusiones a otros organismos similares, participación en botnets, defacements u otras campañas específicas.

• Análisis del hacktivismo en México, incluyendo operaciones actuales, objetivos e impacto, proporcionando recomendaciones de protección.

• Análisis de correos electrónicos o sitios web sospechosos, incluyendo identificación de encabezados, análisis de *malware*, extracción de datos y evaluación de riesgo en una plataforma de Inteligencia sobre Amenazas.

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

El proveedor deberá de reportar al Instituto cada vez que se genere un evento de ciberinteligencia, detallado los hallazgos y las acciones de prevención y/o contención que deberán realizarse, incluyendo portales públicos expuestos en Internet, cuentas de correo electrónico institucionales o de aplicación comprometidas, suplantación de identidad o daño a la imagen institucional.

Para aquellos portales que se encuentren en el supuesto de suplantación de identidad, daño a la imagen o reputación institucional o sospecha en el manejo de datos sensible de información (venta de datos o información institucional, uso de imágenes o logos institucionales), el proveedor deberá iniciar un proceso

de solicitud de baja al o los proveedores de servicios donde se hospedan estos sitios (takedown), así como iniciar un proceso de notificación al Instituto para que se realicen las notificaciones formales a socios de negocio que apoyen el proceso de ciberpatrullaje (CERTs de otros organismos públicos y/o privados).

iv.2.5 Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos Móviles.

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

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

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

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

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

• Cifrado TKIP y AES basado en hardware.

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

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

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

• Permitir la instalación de aplicaciones y ejecutar actualizaciones en múltiples dispositivos a la vez de manera remota y controlando el tipo de conexión y la fecha de ejecución.

• Permitir realizar modificaciones de cambio de contraseña de bloqueo, y también se puede configurar la longitud, el tipo de contraseña, si es alfanumérica o numérica, el número de intentos, entre otros.

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

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

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

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

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

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

• Alarmas.

iv.2.6 Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA).

Descripción del servicio: El Instituto requiere de un servicio de control de acceso para usuarios privilegiados con el objetivo de brindar funcionalidades de control y monitoreo de las cuentas de usuarios privilegiados en sus servidores, así como implementar un sistema de Autenticación, Autorización y Contabilización (AAA, por sus siglas en inglés: Authentication, Authorization and Accounting). Por lo tanto, el proveedor seleccionado deberá cumplir con las siguientes especificaciones funcionales mínimas:

• Dar continuidad operativa a la solución tecnológica que permita un control detallado del acceso a los activos de infraestructura que respaldan las aplicaciones, mediante la administración del ciclo de vida de las identidades.

• Integrar procesos que identifiquen los roles y perfiles de cada usuario por aplicación, junto con la capacidad de rastrear los accesos realizados, incluyendo la captura de imágenes de pantalla y la grabación de video de las sesiones de acceso.

• Considerar, entre otras, las siguientes plataformas operativas:

- Microsoft Windows
- Unix
- Linux

• Revisar y validar junto con el Instituto los requisitos para proteger las claves privilegiadas en los servidores donde se implementará el servicio.

• Implementar los agentes proporcionados por la solución en los sistemas operativos respaldados por los fabricantes correspondientes.

• Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona de los Centros de Datos designados por el Instituto.

• Acordar con el personal del Instituto las ventanas de mantenimiento necesarias según el tiempo de implementación requerido.

• Integrar el dispositivo con la consola de administración de la solución y garantizar la integración de la bitácora del dispositivo con la solución de Correlación del proyecto.

• Ofrecer servicios de autenticación, autorización y registro (AAA) para habilitar el control de acceso e identidad en la red del Instituto.

• Habilitar los activos de infraestructura necesarios en esquemas de Alta Disponibilidad (HA).

- Capacidad para generar políticas basadas en reglas y atributos.
- Integración con bases de datos externas como Active Directory y LDAP.
- Capacidad de integrarse con un dominio de Directorio Activo.
- Integración con soluciones de contraseña única.
- Integración con dispositivos de red para aplicar políticas de seguridad basadas en identidad.
- Utilización de los siguientes protocolos de autenticación:
  - CHAP/MSCHAP
  - PAP
  - PEAP
  - EAP-TLS
  - MS-CHAP
  - EAP-MD5
- Generación de políticas de restricción por dispositivo y horario.
- Uso de listas de acceso descargables.
- Capacidad para operar en esquemas de clúster con más de 3 dispositivos funcionando como un solo sistema.
- Funcionalidad para operar en esquemas de procesamiento físico (appliance) o virtualizados.
- Interfaz de administración gráfica basada en web.
- Interfaz de programación para operaciones de actualización, creación, lectura y eliminación de dispositivos, terminales y usuarios en la base de datos interna.
- Funcionalidades de reporte y auditoría.
- Capacidades de monitoreo y diagnóstico de problemas.
- Administración de eventos (logs) exportables.

iv.2.7 Servicio de Antivirus

El proveedor deberá proveer el licenciamiento, instalación, habilitación, configuración, puesta a punto, gestión, monitoreo, soporte y mantenimiento de una solución diseñada para proteger contra amenazas de código malicioso que puedan afectar a los dispositivos de trabajo, servidores, correos electrónicos externos e internos, así como la navegación web hacia Internet. Además, se aplicarán políticas de seguridad con el objetivo de fortalecer los controles para mitigar riesgos, proteger la infraestructura institucional y garantizar la continuidad operativa de las actividades de los usuarios.

ANEXOS
DIVISIÓN DE CONTRATOS

La protección antivirus se llevará a cabo mediante un agente distribuido a los activos de infraestructura requeridos por el Instituto. El proveedor será responsable de asegurar la entrega de dicho agente a los activos de infraestructura especificados por el Instituto. La distribución y administración del agente puede llevarse a cabo tanto en entornos locales (on-premise) como en la nube.

El proveedor deberá tener en cuenta que las actividades de remediación de infecciones por virus serán de su responsabilidad. Por lo tanto, deberá brindar el apoyo necesario mediante la utilización de las funcionalidades proporcionadas por la solución antivirus propuesta como parte del servicio actual. Además, el proveedor deberá notificar al personal designado por el Instituto sobre cualquier actividad sospechosa detectada, ya sea a través de correo electrónico u otro medio acordado por ambas partes. Asimismo, deberá ocuparse de atender los incidentes de *malware* según lo estipulado en los Acuerdos de Nivel de Servicio o los Acuerdos de Nivel Operativo.

En el caso de que la instalación requerida por el Instituto supere los 200 agentes, el proveedor, en colaboración con el Instituto, deberá establecer una estrategia para implementar el agente antivirus y garantizar la actualización de este en todos los activos de infraestructura solicitados, sin que ello afecte el funcionamiento del Instituto. Es importante considerar que estos activos y consolas de administración podrán estar distribuidos en diferentes localidades del Instituto.

El proveedor deberá configurar las políticas de seguridad base en la solución antivirus propuesta, las cuales se definirán en conjunto con el Instituto como parte de las reglas que regirán el servicio. Estas políticas deberán ser desplegadas en los activos de infraestructura correspondientes a través de la consola de administración de la solución. Además, el proveedor deberá ajustar estas políticas según sea necesario, basándose en el monitoreo continuo de la solución y en los requerimientos del Instituto.

Se requerirá que el proveedor y el Instituto definan una estrategia para la entrega de actualizaciones de antivirus en todos los activos de infraestructura, asegurando que no se vean afectadas las operaciones de los servicios internos, los cuales están distribuidos en diferentes localidades a nivel nacional. El proveedor será responsable de mantener actualizados en todo momento los activos de infraestructura con la última versión o actualización de antivirus proporcionada por el fabricante.

Además, el proveedor, en colaboración con el Instituto, determinará la cantidad de activos de infraestructura que constituirán la línea base para el primer año de prestación del servicio. Posteriormente, un mes antes de cumplir cada año de servicio, se llevará a cabo una redefinición de esta línea base para el próximo año.

El proveedor deberá suministrar al personal del Instituto la última versión del agente de antivirus para su integración en la imagen de software de los Puestos de Servicio.

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

•Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Antivirus.

•Monitorear el cumplimiento de las políticas de uso de información implantadas en la solución.

•Notificar sobre las actividades sospechosas relacionadas con la infección de activos de infraestructura.

•Notificar sobre todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la Solución de Antivirus, efectuando la contención de estas a través de la solución propuesta.

•Resolver las solicitudes de soporte técnico especializado, a fin de evitar y prevenir infecciones en los activos de infraestructura donde se encuentre instalada la solución de Antivirus.

•Recolectar e integrar, al menos la información de eventos de seguridad o logs generada por la solución de Antivirus, hacia la solución de correlación de eventos, cuyo detalle de información a integrar será definido entre el Instituto y el proveedor.

•Desarrollar la afinación de la solución con base en el resultado del monitoreo continuo, además de gestionar las reglas antivirus en los activos de infraestructura, con base en las necesidades del Instituto y en el resultado del monitoreo día a día.

iv.2.8 Servicios de Prevención de Pérdida de Información

Descripción del servicio: El Instituto requiere una solución para detectar y prevenir la fuga y/o pérdida de información sensible en los activos de infraestructura del IMSS ubicados en los Centros de Datos. Esta solución debe estar integrada con los activos de infraestructura, el servicio de correo electrónico externo, el correo electrónico interno, la navegación web y los portales de colaboración, lo que permitirá una visión completa y una prevención efectiva en múltiples capas de seguridad.

El módulo debe tener la capacidad de establecer políticas mediante el uso de palabras clave o expresiones regulares que identifiquen información sensible, bloqueando su transmisión a través de diferentes canales de comunicación.

El servicio se enfocará en prevenir la fuga de información sensible desde los puestos de servicio.

El proveedor deberá configurar en la solución propuesta las políticas base de seguridad definidas en colaboración con el Instituto, adaptándolas a los activos de infraestructura y creando los perfiles correspondientes.

Estas políticas se desplegarán a través de la consola de administración de la solución, y el proveedor será responsable de ajustarlas mediante un proceso de puesta a punto continuo, basado en su monitoreo constante y los requisitos específicos del Instituto. Para este fin, el Instituto requiere que se tomen en consideración, al menos, las siguientes premisas:

• **Tipos de documentos:** Este apartado abarca las diversas formas en que se pueden estructurar los activos de información relevantes para los procesos del Instituto. Incluyen, entre otros, reportes, estudios, oficios, correspondencia, acuerdos, directivas, planes estratégicos, contratos, convenios, anotaciones, memorandos, estadísticas, procedimientos, políticas, reglamentos, informes, solicitudes, encuestas, históricos y otros documentos similares.

• **Medios de almacenamiento de la información:** Este apartado hace referencia a los diferentes medios disponibles para resguardar los activos de información con el propósito de manipularlos en el futuro.

El proveedor deberá garantizar que las funcionalidades de la Solución de Prevención de Pérdida de Información se cumplan incluso si el activo de infraestructura no está asociado a ningún Directorio Activo o a la red del Instituto.

ANEXOS
DIVISIÓN DE CONTRATOS

En el marco de la operación del servicio, el proveedor deberá:

• Emitir alertas de incidentes y vigilar los eventos generados por los componentes tecnológicos de la solución de Prevención de Pérdida de Información.

• Supervisar el cumplimiento de las políticas de uso de la información establecidas en la solución.

• Informar al Instituto sobre actividades sospechosas relacionadas con la violación de las políticas de fuga de información configuradas en los activos de infraestructura.

• Implementar medidas de contención ante actividades sospechosas.

• Atender las solicitudes de soporte técnico especializado para prevenir fugas de información en los equipos donde esté habilitada la solución.

• Recopilar e integrar, al menos, la información de eventos de seguridad o registros generados por la solución de Prevención de Pérdida de Información en la solución de correlación de eventos, cuyo alcance será definido entre el Instituto y el proveedor.

• Gestionar los componentes tecnológicos a través de procesos de gestión de cambios, configuraciones y versiones según los requisitos del Instituto.

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

•Presentar un registro de auditoría que contenga todas las actividades realizadas por los usuarios.

• Ofrecer reportes predefinidos y personalizados que puedan ser programados o generados de manera puntual.

• Disponer de un mecanismo de alertas y notificaciones.

• Tecnología de Detección:

- Capacidad para extraer texto de diversos tipos de documentos para llevar a cabo análisis de contenido.
- Habilidad para realizar detecciones basadas en palabras clave o frases clave personalizadas, con la capacidad de combinar múltiples palabras en una sola regla de detección.

• Capacidad para realizar análisis de contenido en varios canales de información (correo electrónico, HTTPS/HTTP, FTP, entre otros).

iv.2.9 Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)

El servicio tiene como objetivo asegurar la continuidad operativa del Sistema de Gestión de Seguridad de la Información (SGSI), el cual debe estar alineado con el estándar ISO/IEC 27001:2022. Este sistema se encargará de emitir directivas relacionadas con la seguridad de la información tanto a las áreas de TI como a los terceros responsables de apoyar la operación de TI. Es fundamental que este servicio sea

adaptable a las actualizaciones necesarias para mantener la conformidad con las últimas versiones y requisitos normativos.

El proveedor del servicio deberá garantizar la continuidad operativa del mismo, ofreciendo al menos las siguientes funcionalidades operativas:

Planificación:

Capacitación de seguimiento: Se llevará a cabo un curso de "Inducción a la norma ISO/IEC 27001:2022 o la versión vigente", con el objetivo de proporcionar a los participantes las habilidades necesarias para:

- Comprender la estructura de la norma ISO/IEC 27001:2022.
- Interpretar los requisitos necesarios para el cumplimiento de dicha norma.
- Conocer las etapas fundamentales para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).
- Se contempla la participación de al menos 8 personas, con una duración mínima de 8 horas y máxima de 40 horas.

Seguimiento y actualización en la aplicación de las directivas en materia de seguridad: Revisión y actualización del Manual de Políticas de Seguridad de la Información que cumplirá con los siguientes criterios:

- Cubrir los dominios establecidos por la norma ISO/IEC 27001:2022.
- Incluir los procesos de seguridad aplicables según la normativa actual.
- Estar dirigido tanto a las áreas de TI como a los terceros que prestan servicios de TI al Instituto, abordando al menos 20 directivas relacionadas con el catálogo de infraestructuras críticas del Instituto.

Identificación y evaluación de activos (relacionados con el catálogo de infraestructuras críticas) del proceso involucrado en el Sistema de Gestión de Seguridad de la Información.

La metodología que seguir deberá contemplar los siguientes aspectos:

- Identificación de los activos del proceso.
- Valoración de los activos del proceso.
- Identificación de los requisitos de seguridad.
- Identificación de los controles de seguridad existentes.

Generación de la Declaración de Aplicabilidad (SoA: Statement of Applicability).

La metodología deberá abordar los siguientes aspectos:

- Identificación y evaluación de la aplicabilidad de los requerimientos internos y externos.
- Selección de los objetivos de control y los controles para mitigar los riesgos.
- Verificación de los requisitos contractuales y legales.
- Identificación de los requisitos internos y externos pertinentes.
- Validación de la aplicabilidad de los requisitos identificados.
- Elaboración del Formato de Autorización para la implementación y operación del Sistema de Gestión de Seguridad de la Información.
- Preparación de la Declaración de Aplicabilidad.

ANEXOS
DIVISIÓN DE CONTRATOS

- Documentación de los objetivos de control, los controles seleccionados y la justificación de su elección.
- Documentación de los controles actualmente implementados.
- Documentación de la exclusión de controles y la justificación de dicha exclusión.

Operación del Sistema de Gestión de Seguridad de la Información

- Análisis de Riesgos de Seguridad de la Información
- Análisis de riesgos basado en el servicio definido de gestión de riesgos de seguridad.
- Generación y actualización del plan de tratamiento de riesgos.

La metodología debe considerar los siguientes aspectos:

- Identificación de las acciones a realizar por parte de la institución y su administración.
- Identificación de los recursos necesarios y establecimiento de prioridades.
- Asignación de responsabilidades para la gestión de riesgos de seguridad de la información.

Aplicación del seguimiento al plan de tratamiento de riesgos.

La metodología deberá considerar los siguientes aspectos:

- Asignación de roles y responsabilidades para supervisar los controles relacionados con personas, procesos y tecnología involucrados en la mitigación de los riesgos.
- Actualización de la documentación, conforme 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 abordar los siguientes temas:

- Control de accesos.
- Monitoreo de cuentas.
- Definición del proceso de Continuidad del Negocio.
- Implementación de los roles y responsabilidades definidos para el Sistema de Gestión de Seguridad de la Información.
- Controles de seguridad en la infraestructura tecnológica, conforme a lo establecido en el alcance.

Gestión del cambio cultural.

La metodología debe abordar los siguientes aspectos:

- Actualización del Programa de Concientización dirigido a usuarios y operadores del Sistema de Gestión de Seguridad de la Información.
- Seguimiento y apoyo a las necesidades de capacitación del personal encargado de administrar el Sistema de Gestión de Seguridad de la Información y de la seguridad de la información.

- Elaboración o actualización del Manual de Gestión de Seguridad de la Información. Este manual deberá incluir las referencias generadas en esta fase para garantizar la trazabilidad de las cláusulas de la norma.

Monitoreo y revisión del Sistema de Gestión de Seguridad de la Información.

La metodología deberá abordar los siguientes aspectos:

- Los responsables del proceso deben realizar una revisión y actualización del Sistema de Gestión de Seguridad de la Información para garantizar que los objetivos de este sistema estén alineados con los objetivos de negocio en materia de seguridad de la información, y que aseguren el manejo adecuado de los riesgos existentes.
- El proveedor debe actualizar el procedimiento de las revisiones gerenciales.
- Asimismo, el proveedor deberá actualizar los formatos necesarios para llevar a cabo las revisiones gerenciales.

Auditorías internas.

La metodología deberá abarcar lo siguiente:

- Seguimiento y apoyo en la elaboración del plan de auditorías internas para las áreas de TI y para los terceros que proporcionan servicios de TI al Instituto.
- Actualización o, en su caso, definición de los formatos necesarios para llevar a cabo las auditorías.
- Ejecución de una auditoría interna del Sistema de Gestión de Seguridad de la Información para verificar el cumplimiento con el estándar ISO/IEC 27001:2022 o la normativa vigente, así como con los procesos establecidos en la normativa aplicable.

Actualización del Sistema de Gestión de Seguridad de la Información e Implementación de Mejoras

Deberá considerar los siguientes aspectos:

- Priorización de las acciones correctivas y de las no conformidades identificadas en las revisiones gerenciales, revisiones independientes, auditorías internas y revisiones técnicas.
- Identificación de los responsables encargados de llevar a cabo las mejoras.
- El Instituto establecerá fechas de compromiso para la finalización de las mejoras, exclusivamente para seguimiento interno.

Acciones Correctivas y No Conformidades

Deberá tener en cuenta lo siguiente:

- Apoyo en la definición y seguimiento del procedimiento para llevar a cabo acciones correctivas y atender no conformidades derivadas de las auditorías.
- Actualización del formato para el registro de acciones correctivas y no conformidades.
- Coordinación de la ejecución de las acciones correctivas ya definidas y, en caso necesario, de las no conformidades identificadas.

Comunicación de los Resultados de las Acciones Tomadas

ANEXOS
DIVISIÓN DE CONTRATOS

Se deberán considerar los siguientes puntos:

- Apoyo en la programación de reuniones de seguimiento al Sistema de Gestión de Seguridad de la Información, con el fin de informar sobre el alcance de las acciones correctivas y las no conformidades abordadas, y verificar su cumplimiento con los requisitos de los propietarios de la información y de los involucrados en los procesos del Instituto.

iv.2.10 Servicios Continuidad de Gestión del Cambio en Seguridad de la Información

Descripción del Servicio: El Instituto requiere la implementación de un programa de gestión del cambio para fortalecer la protección de la información, en consonancia con los requisitos del estándar ISO/IEC 27001:2022, mediante una estrategia cultural.

Este servicio deberá incluir un plan exhaustivo de transferencia de conocimientos al personal del Instituto sobre los principales aspectos de seguridad de la información, abarcando al menos los siguientes ámbitos:

- Regulación actual en materia de seguridad de la información.
- Políticas de seguridad específicas del Instituto.
- Procesos relacionados con la seguridad en el Instituto.
- Controles de seguridad implementados en el Instituto.

El servicio se estructura en las siguientes etapas:

Etapa 1: Definición de la Estrategia de Gestión del Cambio

- Contextualización del Instituto: El proveedor deberá comprender el contexto cultural del Instituto en lo que respecta a la seguridad de la información.
- Diagnóstico del Estado Actual: El proveedor realizará un análisis para evaluar el nivel de conocimiento existente en seguridad de la información, identificando las brechas entre la situación actual y los requisitos establecidos por el Instituto.
- Preparación de la Estrategia: Basándose en los resultados del diagnóstico, el proveedor propondrá una estrategia de gestión del cambio en seguridad de la información para facilitar una transferencia efectiva de conocimientos.

Etapa 2: Diseño del Programa de Gestión del Cambio

- Preparación del Programa: El proveedor elaborará un plan de trabajo detallado que incluirá los temas a abordar en la transferencia de conocimientos, el número de personal involucrado y las fechas de implementación.
- Elaboración de Contenidos: El proveedor desarrollará materiales en formato PowerPoint u otros definidos por el Instituto, que serán utilizados para la transferencia de conocimientos en seguridad de la información.
- Creación del Modelo de Evaluación: El proveedor presentará un modelo de evaluación destinado a medir la efectividad de la transferencia de conocimientos en seguridad de la información.
- Preparación del Grupo de "Train the Trainers": El proveedor identificará y preparará a un grupo de 5 facilitadores con el fin de que puedan replicar la transferencia de conocimientos en otras áreas clave dentro del Instituto.

Etapa 3: Comunicación del Programa de Gestión del Cambio

- Implementación de la Transferencia: El proveedor ejecutará la transferencia de conocimientos al personal de Tecnologías de la Información del Instituto y a las áreas definidas por este, ubicadas en la Ciudad de México.

Etapa 4: Medición del Programa de Gestión del Cambio

- Implementación de Evaluaciones: El proveedor pondrá en marcha una herramienta tecnológica para realizar evaluaciones en línea a los participantes de la transferencia de conocimientos.
- Análisis de Datos: El proveedor analizará la información recopilada para organizar los resultados obtenidos.
- Presentación de Resultados: El proveedor llevará a cabo una presentación ejecutiva ante el personal de Tecnologías de la Información del Instituto, en la que se expondrán los resultados generales obtenidos.

iv.2.11 Servicios del Centro de Operaciones de Seguridad (SOC)

El Instituto requiere que el proveedor del servicio cuente con un Centro de Operaciones de Seguridad (SOC) que esté físicamente ubicado en las instalaciones del proveedor. El propósito de este centro deberá ser garantizar la continuidad operativa y gestionar la seguridad, así como encargarse de la administración, operación, monitoreo, soporte y resolución de fallas de los componentes de las soluciones de seguridad. Esto implica llevar a cabo actividades como revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, y establecimiento de acciones para mejorar de manera sostenible.

El servicio del Centro Operaciones de Seguridad (SOC), que respaldará la operación y prestación del servicio requerido por el Instituto debe ofrecer un control continuo, mayor eficiencia y oportunidad de mejora. Para lograr esto, el licitante debe proporcionar servicios de tecnología de la información confiables en lo que respecta a la gestión de servicios de TI. Estos servicios deben estar respaldados por certificaciones ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018 vigentes y emitidas a nombre del o los licitantes participantes, en caso de presentar una propuesta de participación individual o conjunta.

El licitante deberá tener en cuenta que el servicio de SOC se refiere a las soluciones propuestas e implementadas actualmente por el instituto. Además, deberá considerar que la correlación de bitácoras se basará en un servicio de correlación de eventos e incidentes de seguridad en el que los casos de uso deben ser ilimitados. Asimismo, las respuestas a incidentes deben estar alineadas con los niveles de servicio (SLA) establecidos para este servicio, garantizando tiempos de respuesta adecuados.

El Centro de Operaciones de Seguridad (SOC) debe estar ubicado en el territorio nacional, lo cual se puede verificar con una copia simple de las certificaciones ISO/IEC27001:2022 e ISO/IEC20000-1:2018 a nombre del proveedor participante. Este SOC debe cumplir con las siguientes especificaciones:

- Funcionamiento continuo las 24 horas del día, los 7 días de la semana, los 365 días del año (7x24x365), de acuerdo con lo establecido en el contrato.
- Disponibilidad de personal cualificado para brindar atención tanto en el lugar como de forma remota, con las credenciales necesarias para administrar y monitorear los componentes de la solución.
- Operación en un centro de datos alternativo ubicado en el territorio nacional.
- Mantenimiento de suscripciones a sitios y listas de empresas, fabricantes y medios especializados en seguridad de la información para detectar nuevas vulnerabilidades.

ANEXOS
DIVISIÓN DE CONTRATOS

- Infraestructura dedicada para la gestión, operación y monitoreo de los componentes de hardware y software de los servicios de seguridad.
- Ejecución de evaluaciones operativas a los servicios (software y activos de infraestructura) cada 3 meses desde el inicio de operaciones y hasta 3 meses antes de la finalización de estos, con el fin de identificar mejoras en el rendimiento, la gestión de configuraciones y nuevas funcionalidades.
- Implementación de acciones correctivas y preventivas para garantizar la confidencialidad, integridad y disponibilidad de la información manejada en las soluciones de seguridad.
- Envío de notificaciones y alertas personalizadas en caso de desviaciones, anomalías o brechas de seguridad para cada solución de seguridad.
- Revisiones continuas de la operación del SOC para mejorar procesos, procedimientos y controles de seguridad.
- Análisis de eventos de seguridad y registros de administración integrados en los servicios de correlación de información para establecer acciones preventivas mediante modificaciones en las configuraciones de las soluciones de seguridad.
- Integración de un Equipo de Atención y Respuesta a Incidentes de Seguridad.
- Soporte y atención a fallas de los componentes de hardware y software de la solución según lo establecido en los acuerdos de niveles de servicio.
- Monitoreo de la disponibilidad de los componentes hardware y software de la solución, con capacidad para generar alertas y notificaciones en caso de fallos, degradación del rendimiento, intermitencia o pérdida de disponibilidad.
- Mantenimiento preventivo y correctivo de las soluciones de seguridad habilitadas y los activos de infraestructura que respaldan cada servicio.
- Ejecutar procesos operativos para al menos los siguientes rubros:

  - Gestión de Riesgos
  - Gestión de Continuidad
  - Monitoreo y Detección
  - Gestión de Seguridad de la información
  - Administración de Dispositivos
  - Gestión de solicitudes de servicio
  - Administración de Cambios Operacionales
  - Administración de Configuraciones
  - Administración de Vulnerabilidades
  - Gestión de Incidentes
  - Gestión de Problemas

• Integración de una Mesa de Servicio conforme a las prácticas de ITIL v4, la cual deberá ser compatible con la Mesa de Servicios Tecnológicos del Instituto. Esta integración debe abarcar todas las actividades relacionadas con la configuración, desarrollo de software, ajustes, y otras tareas necesarias para facilitar la comunicación y el intercambio de requerimientos, cambios, incidentes y otros procesos determinados por el Instituto.

• El servicio de gestión de requerimientos, cambios, incidentes y otras solicitudes deberá permitir la creación de eventos (tickets) a través de los mecanismos definidos en las mesas de trabajo correspondientes, los cuales incluyen, de manera ejemplificativa pero no limitativa:

  - Un número telefónico directo en las instalaciones del SOC.
  - Un número telefónico de diez dígitos.
  - Correo electrónico.
  - Portal web.

• El Instituto se reserva el derecho de solicitar la revisión de la infraestructura de seguridad por un tercero en cualquier momento durante la vigencia del contrato, con el fin de asegurar la entrega adecuada del servicio.

• Supervisión de la Base de Datos de la Gestión de la Configuración (CMDB, por sus siglas en inglés), la cual contendrá los detalles pertinentes de cada elemento de configuración (CI) y sus relaciones, abarcando equipos físicos, software, y las interconexiones entre incidencias, problemas, cambios y demás datos del servicio de seguridad.

• Generación de informes de Inteligencia de Negocios y Análisis de Información para obtener estadísticas sobre el uso y rendimiento de los servicios de seguridad. Esto tiene como objetivo respaldar la toma de decisiones estratégicas y operativas, así como determinar el plan de capacidad para cada tecnología implementada. Estos informes pueden incluir, entre otros datos, lo siguiente:

- Estadísticas de utilización de procesamiento por tecnología.
- Estadísticas de rendimiento por tecnología (throughput).
- Estadísticas de ataques informáticos bloqueados.
- Estadísticas de comportamientos típicos esperados por tecnología (líneas base).
- Estadísticas de usuarios concurrentes por servicio.
- Estadísticas de crecimiento diario, mensual y anual para cada servicio.

• Facilitar al Instituto cuentas de acceso a las consolas de administración de los servicios de seguridad, así como proporcionar herramientas de software que permitan acceder a estas consolas (ya sea mediante aplicaciones cliente-servidor, portales web u otros medios disponibles). Estas cuentas deberán tener únicamente permisos de lectura, y los atributos de consulta se definirán en las reuniones establecidas con ese fin.

• Las consolas de administración proporcionadas para los servicios de seguridad deberán permitir visualizar, como mínimo:

- 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. Estas bases de datos deben contener información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licencias adquiridas para cada servicio proporcionado, y cualquier otra información relevante que facilite la toma de decisiones con respecto al uso de los servicios de seguridad.

• Dar continuidad operativa al Tablero de Estadísticas de Servicios de Seguridad a través de un portal único de administración de los servicios de seguridad, independiente de las consolas de administración y herramientas de monitoreo. Este tablero proporcionará información estratégica en tiempo real y de manera histórica sobre el uso de los servicios, permitiendo al Instituto obtener una visión general del rendimiento de las soluciones, su estado de salud, incidentes registrados, reportes de actividades sospechosas relevantes a nivel mundial, u otra información pertinente para la toma de decisiones sobre las condiciones

ANEXOS
DIVISIÓN DE CONTRATOS

operativas de los servicios. El licitante deberá incluir en su oferta económica los costos asociados al desarrollo para cumplir con este requisito.

• Habilitar al personal designado por el administrador del contrato para generar reportes haciendo uso de todas las variables y funcionalidades de la herramienta de monitoreo. Se proporcionará la opción de parametrizar estos reportes y acceder a ellos a través de una interfaz web.

Partida 2

iv.2.12 Servicios de Análisis de Vulnerabilidades Dinámico

Descripción del servicio: El Instituto requiere asegurar la continuidad operativa de un servicio que permita llevar a cabo análisis técnicos especializados sobre los activos de infraestructura de procesamiento, redes, sistemas y aplicaciones, con el objetivo de identificar vulnerabilidades nuevas o conocidas. Por tanto, el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas:

- Integrar las tareas necesarias para ejecutar análisis de vulnerabilidades en los centros de datos especificados por el Instituto, así como en otras ubicaciones según sea necesario.
- Realizar el seguimiento de los reportes utilizando las herramientas disponibles para complementar los análisis de vulnerabilidades realizados.
- Renovar el licenciamiento del *software* necesario para continuar con los servicios y activos de infraestructura pertinentes.
- Garantizar que las herramientas de análisis de vulnerabilidades cuenten con la última versión liberada, estable y validada por el fabricante, así como otros componentes necesarios para el servicio.
- Identificar los servicios a analizar, incluyendo el número de equipos involucrados y la versión de las plataformas de los sistemas.
- Identificar vulnerabilidades documentadas en organismos internacionales como el CVE (Common Vulnerability Exposures).
- Identificar configuraciones por omisión.
- Tener la capacidad para evaluar el grado de vulnerabilidad ante técnicas de ataque como SQL injection, Cross Site Scripting, Cross Site Request Forgery, Sensitive Data Exposure, Security Misconfiguration, y Broken Authentication and Session Management.
- Realizar Análisis de Vulnerabilidades de caja negra, gris o blanca, conforme las solicitudes por evento que genere el Instituto.
- Elaborar un reporte ejecutivo y técnico para cada requerimiento atendido, describiendo los detalles de los riesgos asociados a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP denominada "OWASP Risk Rating Methodology", e incluyendo recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.
- Implementar un proceso y/o procedimiento para garantizar la continuidad de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada, mismo que será proporcionado al personal técnico del Instituto para que este realice las actividades de remediación correspondientes
- Integrar un tablero que contenga las vulnerabilidades detectadas, descripción, clasificación de criticidad e impacto de cada vulnerabilidad (CVE, CVSS, u otros marcos de clasificación), que permitan relacionarlo con cada aplicativo, sistemas o activo de información que haya sido sometido verificación de seguridad.

iv.2.13 Servicios de Análisis de Vulnerabilidades Estático

Descripción del servicio: El Instituto busca evaluar el nivel inicial de madurez de sus prácticas de seguridad en el software y requiere un proveedor que cumpla con las siguientes especificaciones funcionales mínimas:

- Implementar una solución tecnológica centralizada que permita realizar pruebas dinámicas y estáticas, con soporte para los lenguajes de programación como HTML, Java, .Net, C#, PHP.
- Integrar el licenciamiento del software necesario, incluyendo renovaciones durante la vigencia de los servicios.
- Garantizar el uso de las últimas versiones estables y validadas de las herramientas propuestas, así como de otros componentes necesarios.
- Incorporar un proceso de evaluación de las prácticas existentes de seguridad de software en el Instituto.
- Desarrollar un programa de evaluación de seguridad de software con iteraciones definidas en conjunto con el Instituto.
- Actualizar y establecer procesos en las diferentes etapas del ciclo de vida de desarrollo de software para garantizar la seguridad de este.
- Asistir en el cumplimiento de estándares y marcos normativos previamente definidos.
- Identificar el nivel inicial de madurez de las prácticas de seguridad en el software del Instituto.
- Comprender el entorno del Instituto, incluyendo personal, normativas y tecnologías relevantes, para diseñar el modelo de operación y flujos de interacción necesarios.
- Integrar las mejores prácticas de seguridad en el software, alineadas con OpenSAMM.
- Realizar Análisis de Vulnerabilidades estático de caja negra, gris o blanca, conforme las solicitudes por evento que genere el Instituto.
- Transferir las prácticas de seguridad en el software implementadas al personal designado por el Instituto.
- Operar el modelo de madurez establecido, certificando el nivel de cumplimiento del software evaluado en tres etapas: al inicio, durante y posterior al desarrollo de una aplicación.
- Preservar la integridad y confidencialidad de la información recibida durante las pruebas.
- Elaborar un reporte ejecutivo y técnico por cada requerimiento atendido, detallando los riesgos asociados a cada hallazgo o vulnerabilidad identificada, así como recomendaciones y acciones específicas para remediarlas.

iv.2.14 Servicios de Pruebas de Penetración

Descripción del servicio: El Instituto requiere mantener un servicio que asegure un proceso sistemático para verificar las vulnerabilidades de las aplicaciones y la infraestructura que las respaldan, con el objetivo de detectar posibles brechas o fallos en la seguridad. Para cumplir con este propósito, el proveedor deberá atender las siguientes especificaciones funcionales mínimas:

- Integrar todas las actividades necesarias para ejecutar pruebas de penetración en los centros de datos designados por el Instituto, así como en otras ubicaciones según sea necesario.
- Realizar un seguimiento detallado de los servicios o activos de información que se someterán a análisis, incluyendo la cantidad de equipos involucrados y las versiones de las plataformas de los sistemas examinados.
- Identificar vulnerabilidades y configuraciones incorrectas.
- Realizar prueba de penetración de caja negra, gris o blanca, conforme las solicitudes por evento que genere el Instituto.
- Explotar posibles accesos a los sistemas aprovechando las brechas de seguridad y/o vulnerabilidades detectadas.

ANEXOS
DIVISIÓN DE CONTRATOS

- Evaluar vulnerabilidades en áreas como autenticación y autorización, gestión de sesiones, inyección de código, criptografía, ataques lógicos, protección de datos y divulgación de información.
- Evaluación de vulnerabilidades de al menos los siguientes ámbitos:

- 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

- Elaborar informes ejecutivos y técnicos para cada requisito atendido, utilizando la metodología de cálculo de riesgos de OWASP, detallando los riesgos asociados a cada vulnerabilidad identificada y proporcionando recomendaciones y acciones específicas para su corrección.
- Implementar un proceso o procedimiento para garantizar la continuidad de las medidas de remediación y las recomendaciones derivadas de cada revisión realizada.
- Integrar un tablero que contenga las vulnerabilidades detectadas, descripción, clasificación de criticidad e impacto de cada vulnerabilidad (CVE, CVSS, u otros marcos de clasificación), que permitan relacionarlo con cada aplicativo, sistemas o activo de información que haya sido sometido verificación de seguridad.

iv.2.15 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, mediante la integración de registros o bitácoras, las evidencias o indicios de eventos y su relación temporal. Este análisis debe identificar cuándo ocurrió un incidente, qué infraestructura, servicios tecnológicos o sistemas de información se vieron comprometidos, cómo se llevó a cabo y quién o qué estuvo relacionado con el incidente, así como el impacto del evento. Para cumplir con estos objetivos, el proveedor deberá satisfacer las siguientes especificaciones funcionales mínimas:

- Integrar las tareas necesarias para llevar a cabo análisis forenses en los centros de datos designados por el Instituto, así como en otras ubicaciones según sea necesario.
- Continuar con la definición de objetivos, parámetros y cuestionarios relevantes para cada investigación solicitada.
- Mantener un seguimiento continuo de los casos solicitados y registrar los indicadores correspondientes.
- Preservar la integridad de la información recibida durante la ejecución del proceso de análisis forense, asegurando una cadena de custodia adecuada.
- Participar en entrevistas con los principales involucrados para obtener el contexto necesario en las investigaciones digitales.
- Obtener información de fuentes públicas en la red, si es relevante para la investigación realizada.
- Realizar evaluaciones de información en diversos dispositivos y equipos, como computadoras, servidores físicos y virtuales, dispositivos móviles y equipos de comunicaciones, para identificar indicios de compromiso y su evidencia correspondiente.
- Llevar a cabo un proceso de recuperación de información que haya sido borrada previamente.
- Mantener y dar seguimiento a una herramienta colaborativa diseñada para facilitar la visualización de hallazgos a los usuarios finales, así como para generar informes de hallazgos cuando sea necesario.
- Elaborar un dictamen técnico para cada requerimiento atendido, con la información identificada en los procesos de análisis forense, generando y firmando documentos que expresen los

ANEXOS
DIVISIÓN DE CONTRATOS

resultados de la investigación de manera clara y concisa, para que puedan ser comprendidos por aquellos que no dominan el lenguaje técnico.

v. Perfil del Proveedor

El licitante deberá demostrar la capacidad y competencia técnica certificada para operar soluciones de seguridad, asegurando su correcto funcionamiento en los sitios requeridos por "EL INSTITUTO". Para cumplir con este requisito, se solicita presentar una copia simple del acta constitutiva que acredite al menos cinco años de actividad empresarial en el rubro de proveeduría de servicios de seguridad de la información o áreas relacionadas, de acuerdo con las características y especificaciones establecidas en el presente Anexo Técnico.

El personal responsable de las operaciones de los servicios de seguridad debe contar con experiencia demostrada en tecnología y seguridad de la información. Para cumplir con este requisito, se solicita la presentación de los currículos vitae de todos los recursos humanos involucrados en el servicio, los cuales deben incluir al menos:

- Experiencia profesional: Se evaluarán todos los puestos anteriores de cada miembro del equipo, detallando las fechas, nombres de los empleadores, títulos de los puestos y las responsabilidades asociadas. Se exigirá una experiencia mínima comprobada de tres años.
- Experiencia en proyectos especializados en Seguridad de la Información: Se deberán mencionar y describir todos los proyectos en los que el personal haya participado, con una experiencia comprobada mínima de tres años en esta área.
- Estudios: Se registrarán todos los estudios relacionados con la seguridad de la información, así como las certificaciones vigentes a la fecha de presentación de la propuesta técnica. Se requerirán certificaciones de tecnología y/o seguridad de tipo "vendor-neutral".
- Estructura del equipo de trabajo: Se proporcionará una descripción de la estructura del grupo de trabajo, detallando las responsabilidades y competencias de cada perfil.
- Los servicios ofrecidos por el o los licitantes deberán estar respaldados por certificaciones ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018 vigentes y emitidas a nombre del o los licitantes participantes, en caso de presentar una propuesta de participación individual o conjunta.

El acta constitutiva que acredite al menos cinco años de actividad empresarial en el rubro de proveeduría de servicios de seguridad de la información o áreas relacionadas y las certificaciones ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018 vigentes y emitidas a nombre del o los licitantes participantes serán indispensable y su ausencia afectaría la solvencia de la propuesta.

A continuación, se enumeran las credenciales y capacidades que deben cumplir los recursos asignados al proyecto:

Partida 1.

Perfil	Certificaciones que acreditar	Experiencia que 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)	Tres años de experiencia en proyectos relacionados con seguridad de la información.	Responsable de la administración, monitoreo y operación de los servicios provistos por el SOC, además de brindar soporte y atención a fallas e incidentes de seguridad.	Al menos 1
Administración y Operación de soluciones y herramientas tecnológicas	Especialista consultor en cada una de las soluciones de seguridad integradas. Se aceptan como documentos comprobables los certificados vigentes obtenidos directamente del fabricante.	Tres años de experiencia en proyectos relacionados con seguridad de la información.	Administrar, operar y monitorear las soluciones de seguridad propuestas.	Al menos 3
Líder de proyecto	PMP (Project Manager Professional) Certificado por PMI o ITIL v4 (Expert o Master)	Tres años de experiencia en proyectos relacionados con seguridad de la información.	Responsable de administrar y coordinar el proyecto	Al menos 1
Operador de la mesa de servicios SOC	ITIL v4 Foundation Certification	Tres años de experiencia participando en proyectos de seguridad de la información.	Personal encargado de las operaciones de soporte de primer nivel, monitoreo de servicios, registro y seguimiento de solicitudes de ventanas de mantenimiento, reporte de fallas y requerimientos.	Al menos 4

Perfil	Certificaciones que acreditar	Experiencia que demostrar	Función	Número de recursos
Arquitecto especializado en redes y seguridad.	CCNP (Cisco Certified Network Professional)	Tres años de experiencia en participación en proyectos de redes y seguridad de la información.	Responsable de la administración, monitoreo y operación de los servicios proporcionados por el SOC en lo referente a servicios de interconexión de red, así como del soporte y la atención a fallas e incidentes que surjan en la interoperabilidad con otros proveedores y/o fabricantes.	Al menos 1

Partida 2.

Perfil	Certificaciones que acreditar	Experiencia que demostrar	Función	Número de recursos
Líder de proyecto	PMP (Project Manager Professional) Certificado por PMI o ITIL v4 (Expert o Master)	Tres años de experiencia participando en proyectos relacionados con seguridad de la información.	Responsable de administrar y coordinar el proyecto.	Al menos 1
Analista de Seguridad	CEH (Certified Ethical Hacker)	Tres años de experiencia participando en proyectos de seguridad de la información.	Responsable de llevar a cabo las revisiones de seguridad en las aplicaciones y la infraestructura, así como de prever, detectar, analizar, contener, erradicar y documentar incidentes de seguridad.	Al menos 2

Perfil	Certificaciones que acreditar	Experiencia que demostrar	Función	Número de recursos
Consultor de Penetración	GPEN (GIAC Certified Penetration Tester) o CEH (Certified Ethical Hacker) o CICP (Core Impact Certified Profesional)	Tres años de experiencia en proyectos relacionados con seguridad de la información.	Llevar a cabo simulacros de ataques a la red de infraestructura o aplicaciones para determinar el alcance de lo que los atacantes pueden acceder y los problemas que podrían ocasionar. Evaluar la seguridad de la infraestructura de red y las aplicaciones mediante el uso de herramientas y técnicas que un atacante podría emplear.	Al menos 1
Consultor Forense de Cómputo	EnCE (EnCase Certified Examiner) o CHFI (Certified Hacker Forensics Investigator)	Tres años de experiencia participando en proyectos relacionados con seguridad de la información.	Analizar la metodología de ataque en caso de una penetración exitosa a la infraestructura, con el fin de determinar cómo se llevó a cabo y cuál fue el alcance del daño, lo que permitirá identificar las medidas preventivas a implementar. Además, debe poseer la capacidad de llevar a cabo investigaciones forenses si fuese necesario.	Al menos 1

vi. Condiciones técnicas de aceptación de entregable

Durante la habilitación, transición y operación de los servicios de seguridad, el Instituto requiere recibir diversos tipos de documentos, informes, artefactos, dictámenes o esquemas que aseguren el buen

ANEXOS
DIVISIÓN DE CONTRATOS

desempeño y continuidad del servicio. Estos documentos deben proporcionar certeza sobre las actividades diarias que el proveedor llevará a cabo bajo la supervisión de los servidores públicos designados por el Instituto para este propósito.

Entregables Generales

Partida 1.

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto	Única Vez	15 días naturales posteriores a la emisión del fallo
	Documento Compromiso de suscripción del acuerdo de niveles operacional (*Operational Level Agreement*, OLA)	Única Vez	15 días naturales posteriores a la emisión del fallo
	Matriz de Escalación	Única Vez	15 días naturales posteriores a la emisión del fallo
	Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	Única Vez	15 días naturales posteriores a la emisión del fallo
Servicios de Seguridad – Continuidad Operativa	Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a las que se le dará continuidad operativa 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 las que se le dará continuidad operativa en los	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	centros de datos o donde lo indique el Instituto		
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad	Única Vez	20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados
Servicios de Seguridad – Verificación/Calidad	Documento con el diseño de Alto Nivel de los servicios de Seguridad a las que se le dará continuidad operativa 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 las que se le dará continuidad operativa 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

ANEXOS
DIVISIÓN DE CONTRATOS

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

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	• Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo		
	Matriz de Escalación Técnica y Organizacional	Única Vez	15 días naturales posteriores a la emisión del fallo
	Procedimiento de operación de la Mesa de Servicios: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	Única Vez	15 días naturales posteriores a la emisión del fallo
	Expedientes Curriculares del personal del SOC	Única Vez	15 días naturales posteriores a la emisión del fallo
Tablero de Estadísticas de Servicios de Seguridad (Portal Único)	Creación de cuentas de acceso en portal único de las soluciones de seguridad	Única Vez	10 días hábiles posteriores al término de la habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo

Partida 2.

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto	Única Vez	15 días naturales posteriores a la emisión del fallo

	Documento Compromiso de suscripción del acuerdo de niveles operacional (*Operational Level Agreement*, OLA)	Única Vez	15 días naturales posteriores a la emisión del fallo
	Matriz de Escalación	Única Vez	15 días naturales posteriores a la emisión del fallo
	Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	Única Vez	15 días naturales posteriores a la emisión del fallo
Servicios de Análisis de Vulnerabilidades Dinámico	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios de Pruebas de Penetración	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios de Análisis Forense	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios de Análisis de Vulnerabilidades Estático	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo

Entregables bajo demanda

El proveedor deberá generar entregables para los servicios de seguridad, que incluyan, pero no se limiten a, los siguientes conceptos:

Partida 1.

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Borrado Seguro de Información	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado.	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicio de Gestión de Dominios	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos.	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicio de Certificados Digitales SSL	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los certificados que se hayan renovado o adquiridos (incluyendo archivo electrónico compreso con la llave publica	Evento	1 día hábil posteriores a la solicitud generada por parte del Instituto

ANEXOS
DIVISIÓN DE CONTRATOS

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	relacionado con los requerimientos)		
Servicios de Sistema de Gestión de Seguridad de la Información	Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicios de Gestión del Cambio en Seguridad de la Información	Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicios del Centro de Operaciones de Seguridad (SOC)	Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad	Evento	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto
	Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad	Evento	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme cada solicitud generada por el Instituto
	Actualización de la matriz de escalación	Evento	5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad y Red
	Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad y red	Evento	5 días hábiles posteriores a la ejecución de la ventana mantenimiento
	Reporte con Estadísticas de uso y desempeño (información analítica)	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	de las soluciones de seguridad y red		
	Reporte Técnico de las configuraciones de las soluciones de seguridad y red	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico de los incidentes presentados en las soluciones de seguridad y red	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Reporte Técnico de los requerimientos registrados en la mesa de servicios	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y red, así como su diagrama de interrelación conforme fueron registrados en la CMDB	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Diagramas de Arquitectura de las soluciones de seguridad y red	Evento	2 días hábiles posteriores a la solicitud generada por parte del Instituto

Partida 2.

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades Dinámico	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado,	Evento	7 días hábiles posteriores a la solicitud generada por parte del Instituto

ANEXOS
DIVISIÓN DE CONTRATOS

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis		
Servicios de Prueba de Penetración	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicios de Análisis Forense	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de	Evento	15 días hábiles posteriores a la solicitud generada por parte del Instituto

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	infraestructura verificados		
Servicios de Análisis de Vulnerabilidades Estático	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada pieza de software (codigo) analizados indicando al menos: aplicativo relacionado, fecha de análisis, código fuente analizado, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto

Entregables Periódicos

El proveedor deberá generar entregables para los servicios de seguridad, los cuales deben abarcar, entre otros aspectos, los siguientes conceptos mínimos:

Partida 1.

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	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido

ANEXOS
DIVISIÓN DE CONTRATOS

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	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 posteriores al cumplimiento del mes vencido
Servicios del Centro de Operaciones de Seguridad (SOC)	Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte de las evaluaciones operativas a los servicios de seguridad implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Reporte que integre el calendario de actualizaciones de versionamiento en *software* de cada servicio implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario

Partida 2.

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades Dinámico Servicios de Análisis de Vulnerabilidades Estático Servicios de Pruebas de Penetración Servicios de Análisis Forense	Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte de las evaluaciones operativas a los servicios de seguridad implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario
	Reporte que integre el calendario de actualizaciones de versionamiento en *software* de cada servicio implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario

Durante la vigencia del contrato, los entregables requeridos deberán ser presentados en formato electrónico (MS Word, MS Excel, PDF), conforme a los plazos establecidos por el Instituto.

Además, el proveedor deberá establecer y mantener un repositorio digital en el que se almacenarán estos entregables como alternativa. Este repositorio estará disponible para consulta durante todo el periodo del contrato. Los permisos de acceso serán definidos por el Instituto durante las reuniones de trabajo, pudiendo ser otorgados al administrador del contrato, al cuerpo de gobierno designado para este propósito, u otros funcionarios designados por el Instituto.

vii. Cronograma de actividades

ANEXOS
DIVISIÓN DE CONTRATOS

ETAPAS	2025											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Planeación												
Estabilización												
Mejora Continua												
Termino												

viii. Niveles de servicio acordados que deberán cumplirse

El propósito de los Niveles de Servicio es proporcionar al Instituto un método para:

- Evaluar de manera efectiva el rendimiento de los servicios proporcionados por el proveedor.
- Garantizar que los servicios sean entregados con la calidad esperada.

Los Niveles de Servicio son indicadores definidos por el IMSS que el proveedor del servicio SASI 2025 deberá cumplir para asegurar la calidad requerida en la prestación del servicio.

En cumplimiento de lo establecido en los artículos 45, fracción XIX, 53 y 53 BIS de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como en los artículos 86 (segundo párrafo), 95, 96 y 97 de su Reglamento, se aplicarán las Penas Convencionales y Deducciones correspondientes por cualquier retraso en las fechas acordadas de entrega o en el inicio de la prestación del servicio, así como por incumplimientos parciales o deficientes en los servicios prestados por el Proveedor del SASI 2025.

La aplicación de los niveles de servicio se regirá de acuerdo con lo establecido en los "Términos y Condiciones".

ix. Requerimientos de arquitectura tecnológica

Para atender a los requerimientos de Arquitectura Tecnológica, deberá remitirse a lo establecido en el presente Anexo Técnico y sus Apéndices A y B.

x. Restricciones e interfaces con otros elementos

No existen restricciones o interfaces con otros elementos para llevar la implementación y/o continuidad operativa de los servicios establecidos en el presente Anexo Técnico y sus Apéndices A y B.

b) Pruebas requeridas, método de evaluación y el resultado mínimo que debe obtenerse al ejecutar las pruebas.

No se requiere ejecutar pruebas previas para los servicios solicitados conforme el Anexo Técnico y sus Apéndices A y B.

c) Modificaciones de la especificación técnica de algún bien que no se encuentre regulado por el compendio nacional de insumos para la salud.

No Aplica

d) Modificaciones de la especificación técnica de un bien respecto de las estipuladas en el ejercicio anterior.

No existen modificaciones técnicas de los servicios conforme las solicitadas en el ejercicio anterior. Sin embargo, el presente Anexo Técnico incluye servicios adicionales conforme las necesidades operativas y en cumplimiento normativo en materia de seguridad de la información.

Normas: Oficial Mexicana, Estándar (antes mexicana), Internacional, de Referencia o Especificación Técnica, que resulte aplicable a los bienes o servicios requeridos.

No Aplica

Normativa aplicable

El Proveedor de servicios estará sujeto a las políticas internas vigentes del Instituto y a cualquier modificación o inclusión de nuevas políticas que se realicen durante la duración del contrato. Estas políticas aplicables se comunicarán durante las mesas de trabajo; sin embargo, deberán tener en cuenta las siguientes, enunciativas, pero no limitativas:

- 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 basadas en el Sistema de Gestión de Seguridad de la Información (SGSI) del Instituto.
- - ISO/IEC27001:2022 e ISO/IEC20000-1:2018

Cumplimiento de Políticas

El Proveedor de servicios deberá adherirse estrictamente a las políticas de seguridad en vigor en el Instituto y garantizar en todo momento el cumplimiento de los lineamientos establecidos. En caso de que alguno de estos lineamientos cambie durante la vigencia del contrato, el Proveedor deberá ajustar su infraestructura y procesos para cumplir con los nuevos requisitos.

Todos los dispositivos informáticos de propiedad del proveedor de servicios, utilizados en la prestación de los servicios, deben estar equipados con sistemas de detección de intrusos, protección contra virus, así como herramientas para detectar y eliminar programas maliciosos como "backdoors" o "troyanos". Esta medida se aplica tanto a dispositivos móviles (laptops, smartphones, tablets, etc.) como a equipos de escritorio (desktop, deskside, etc.) utilizados por el personal asignado para tareas de administración y gestión.

Si estos dispositivos requieren la instalación de sistemas operativos, aplicaciones, antivirus u otras herramientas necesarias para su correcto funcionamiento, así como la adquisición, instalación, mantenimiento y licenciamiento de estos, todos los costos asociados correrán a cargo del proveedor.

Consideraciones a la finalización del contrato

En caso de terminación anticipada del contrato o al finalizar su vigencia, el "proveedor" será responsable de iniciar el proceso de respaldo de la información, realizar el proceso de baja, llevar a cabo los movimientos de resguardo, traslado y empaquetado de todo el equipo ubicado en las instalaciones del IMSS que forma parte de los servicios y que no constituya parte de las modificaciones, adecuaciones y/o activos que hayan sido realizados como permanentes, o aquellos que de común acuerdo con el IMSS hayan sido sustituidos como parte del servicio.

Una vez concluida 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 garantizar la continuidad operativa. Esta transferencia se realizará mediante un acta de entrega recepción, en la que dichos componentes se transmitirán al IMSS, de manera gratuita y libre de toda limitación de dominio, gravamen y responsabilidad de cualquier naturaleza, conforme a la normativa aplicable al Instituto.

El retiro será coordinado con el tercero que resulte adjudicado, es decir al que se entregue el nuevo contrato o la solución que dará continuidad a la operación del IMSS respecto a los servicios de SASI 2025, observando los acuerdos operativos de migración de un contrato a otro, que contemplen aspectos como la migración de la información de usuario actual hacia la nueva solución.

El "proveedor" deberá entregar al IMSS, a más tardar 2 meses antes de la finalización del contrato, un plan de trabajo detallado para lograr una transición efectiva de los servicios de seguridad, en el que se incluyan todos los elementos necesarios para llevarlo a cabo. Dicho plan debe permitir una transición completa y correcta de los servicios, incluyendo la conformación y actualización de la documentación del proyecto, así como las mesas de trabajo necesarias para dicha transición con los proveedores que den continuidad operativa al proyecto.

La documentación deberá incluir información generada durante la vigencia del contrato, documentación de los procesos internos de aprovisionamiento, configuración y tareas de operación, soporte y mantenimiento debidamente actualizadas, considerando los eventos de administración de cambios y configuración, incidentes y problemas, además de un inventario actualizado a la fecha de entrega de todos los componentes habilitadores e infraestructura auxiliar que el IMSS solicite para la transición a un nuevo contrato de servicios, con el fin de continuar prestando el mantenimiento preventivo y correctivo a todos los componentes de la solución y diseñar el mecanismo para la renovación tecnológica del resto, minimizando el impacto en la operación.

La fecha límite para la entrega de la documentación final actualizada será 2 meses antes de la finalización del contrato SASI 2025. Además, el "proveedor" implementará un esquema de respaldo de la información en cada uno de los componentes que integran los servicios, incluyendo los relacionados con los Centros de Datos del IMSS. El respaldo de la información se almacenará en cada punto táctico para ser entregado al cuerpo de gobierno del contrato para su resguardo, una vez obtenida la autorización correspondiente.

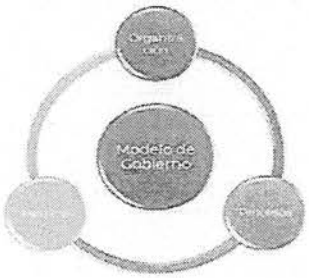
Asimismo, al término del contrato, el "proveedor" garantizará los niveles de servicio durante el período de transferencia de servicios al nuevo proveedor. Dicho período de transición estará sujeto al plan de trabajo previamente presentado por el "proveedor" y aprobado por el IMSS. Durante este período, el "proveedor" proporcionará la orientación tecnológica adecuada al personal del IMSS para garantizar la continuidad de los servicios requeridos, poniendo a disposición del IMSS o de un tercero la transferencia.

Modelo de Gobierno

El Modelo de Gobierno define la estructura operativa y los lineamientos para el proyecto, así como los criterios para evaluar su desempeño. Surgiendo de la necesidad de implementar una estructura orientada a procesos para administrar los "Servicios Administrados de Seguridad Informática SASI 2025", este

modelo facilita la colaboración entre todas las partes involucradas para su implementación y operación eficaz.

Este modelo abarca los aspectos clave para asegurar y supervisar la ejecución del proyecto, incluyendo la organización y los roles del Instituto dentro del mismo. Establece esquemas operativos y procesos para que el administrador del contrato, los líderes del proyecto y el proveedor del servicio (SOC) puedan garantizar los niveles de servicio establecidos en cada etapa de la operación.



La estructura organizacional diseñada para el proyecto de "Servicios Administrados de Seguridad Informática 2025 (SASI)" tiene como objetivo garantizar la eficacia en el trabajo de los responsables, definiendo claramente los roles y responsabilidades en cada nivel. A continuación, se presenta una tabla de manera enunciativa, sin que esto constituya una limitación, que muestra a los responsables y sus roles correspondientes.

e) Firmas de elaboración, revisión y aprobación

Elaboró/Revisó	Cargo	Firma	Fecha
Ing. Abraham Gutiérrez Castillo	Titular de la División de Seguridad Informática Física		01/04/2025

Aprobó	Cargo	Firma	Fecha
Ing. Javier Cortes López	Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información		01/04/2025

f) Relación de Anexos

Id.	*Nombre*	*Descripción corta*	*Fecha de integración al producto*
1	Apéndice "A"	Especificaciones técnicas y operativas	01/04/2025

ANEXOS
DIVISIÓN DE CONTRATOS

2	Apéndice "B"	Inventario de activos de infraestructura	01/04/2025

Control de versiones del documento

Versión	Fecha	Descripción	Responsable
Ver 0.1	31/05/2024	Actualización del Documento	Lic. Cynthia Osmara Verdín Villegas
Ver 0.2	31/05/2024	Revisión del Documento	Ing. Abraham Gutiérrez Castillo
Ver 1.0	31/05/2024	Aprobación del Documento	Lic. Florencio Fernando González Velázquez
Ver 1.1	01/09/2024	Ajustes/Revisión del documento	Ing. Abraham Gutiérrez Castillo
Ver 2.0	01/09/2024	Aprobación del documento	Ing. Javier Cortes López

ANEXOS
DIVISIÓN DE CONTRATOS

Contenido

1. Objetivo del documento 3
2. Vigencia de la contratación y ejercicio presupuestal al que corresponda. 3
3. Plazo de entrega del bien, arrendamiento o servicio. 3
4. Criterio de evaluación. 3
5. Licencias, permisos, registros, certificados o autorizaciones. 3
6. Folletos, catálogos, fotografías, manuales entre otros. 3
7. Visitas a las instalaciones institucionales. 3
8. Lugar de entrega. 3
9. Visitas a las instalaciones del licitante. 3
10. Penas convencionales y deductivas. 4
11. Mecanismos requeridos al proveedor para responder por defectos o vicios ocultos de los bienes o de la calidad de los servicios. 25
12. Garantías de anticipos y cumplimiento. 25
a) Plazo para notificar al proveedor. 25
b) La existencia de consumibles y refacciones, en su caso. 26
c) Plazo y condiciones de canje o devolución del bien. 26
d) Caducidad de los bienes. 26
e) Centros de servicio (domicilios y horarios) y reporte técnico. 26
f) Periodo de garantía. 26
g) Tiempos máximos de reparación o atención de fallas. 26
h) Garantía de mano de obra y/o partes. 26
i) Mantenimientos correctivos y/o preventivos. 26
j) En su caso, si se requiere capacitación, solicitar programa para la misma. 26
k) Porcentaje a requerir por concepto de garantía de cumplimiento. 26
13. Forma de pago. 26
14. Mecanismos de comprobación, supervisión y verificación de los bienes o de los servicios contratados. 27
15. Anticipo. 27
16. Aviso de privacidad y medidas de seguridad para el manejo de la información para bienes o servicios de TIC. 27
17. Seguro de Responsabilidad Civil. 27
18. Dictámenes de protección civil emitidos por las autoridades competentes en la materia. 27
19. Confidencialidad 27
21. Tipo de abastecimiento. 28
22. Modalidad del contrato 28
23. Representante del Área Técnica y Auxiliar del Administrador del Contrato 28
24. Administración de la Contratación 28
25. Representante del Área Requirente de la Contratación 29
26. Firmas de elaboración, revisión y aprobación 29

1. Objetivo del documento

Definir las necesidades y condiciones para la entrega de los "Servicios Administrados de Seguridad Informática 2025.

2. Vigencia de la contratación y ejercicio presupuestal al que corresponda.

La vigencia contractual será a partir del día hábil siguiente a la notificación de la adjudicación y hasta el 31 de diciembre de 2025.

3. Plazo de entrega del bien, arrendamiento o servicio.

El plazo será a partir del día hábil siguiente a la notificación de la adjudicación y hasta el 31 de diciembre de 2025.

4. Criterio de evaluación.

La evaluación de las proposiciones se llevará a cabo utilizando el criterio binario, centrándose exclusivamente en los requisitos establecidos en el Anexo Técnico del servicio y en el formato de propuesta económica. Esto garantizará el cumplimiento satisfactorio de las respectivas obligaciones.

La omisión total o parcial en la presentación de alguno de los rubros a evaluar **SERA** será motivo de desechamiento.

5. Licencias, permisos, registros, certificados o autorizaciones.

El licitante debe incluir en su propuesta una descripción detallada de todos los recursos materiales y humanos requeridos para la prestación de los servicios.

Normas Internacionales.

- Certificado ISO/IEC27001:2022
- Certificado ISO/IEC20000-1:2018

Vigentes y emitidas a nombre del o los licitantes participantes serán indispensables y su ausencia afectaría la solvencia de la propuesta.

6. Folletos, catálogos, fotografías, manuales entre otros.

Los folletos, hojas de especificaciones, y demás documentación técnica, deberán estar integrados como parte de la propuesta del licitante, misma que será verificada a través del dictamen técnico que se emita por parte del Área Técnica.

7. Visitas a las instalaciones institucionales.

No aplica

8. Lugar de entrega.

La entrega se realizará en las instalaciones del Instituto ubicadas en Avenida Paseo de la Reforma 476, Anexo de Telecomunicaciones Planta Alta, Colonia Juárez, Delegación Cuauhtémoc, Ciudad de México, C.P. 06600.

9. Visitas a las instalaciones del licitante.

No aplica

ANEXOS
DIVISIÓN DE CONTRATOS

10. Penas convencionales y deductivas.

- **Penas convencionales**

De conformidad con lo establecido en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como el 85 fracción V, 95 y 96 de su Reglamento, numeral 5.5.8. de las Políticas, Bases y Lineamientos del IMSS, el administrador del contrato llevará a cabo el cálculo y la aplicación de las penas convencionales, según lo estipulado en contrato, notificando al proveedor para proceder con el pago correspondiente.

El proveedor estará sujeto a penas convencionales por cada día hábil de retraso en el cumplimiento de las fechas pactadas de entrega o de la prestación del servicio.

El incumplimiento en la prestación del servicio será determinado por el Administrador del Cumplimiento del contrato, quien calculará y notificará por escrito el monto de la pena convencional al proveedor.

El monto máximo de las penas convencionales por atraso no podrá exceder del monto de la garantía de cumplimiento del contrato y se aplicará sobre el monto total sin incluir el Impuesto al Valor Agregado ni el Impuesto Especial sobre Producción y Servicios.

En ningún caso las penas convencionales podrán negociarse en especie.

Servicios de Habilitación, Operación y Transición

Partida 1 y 2.

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Plan de trabajo detallado de los servicios del proyecto	15 días hábiles posteriores a la emisión del fallo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Documento Compromiso de suscripción de OLAs	15 días hábiles posteriores a la emisión del fallo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Matriz de Escalación	15 días hábiles posteriores a la emisión del fallo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Deberá proporcionar un documento por parte del proveedor, firmado por su representante legal, en el cual se declaren las habilidades,	15 días hábiles posteriores a la emisión del fallo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

competencias y capacidades necesarias para respaldar la prestación de los servicios requeridos.			

Servicios de Seguridad – Continuidad Operativa

Partida 1.

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Documento con el diseño de alto nivel de las soluciones de seguridad a los cuales se dara continuidad operativa 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	1% 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 los cuales se dara continuidad operativa 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	1% 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 después de la finalización de la habilitación de todos los componentes en los Centros de Datos, o en el lugar designado por el Instituto, según lo establecido para cada solución integrada y una vez completada la integración de las mesas de trabajo.	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Memorias técnicas actualizadas de los servicios de seguridad	20 días hábiles antes de la finalización del contrato para aquellos servicios que estén habilitados.	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Servicios de Seguridad – Verificación/Calidad

Partida 1.

ANEXOS
DIVISIÓN DE CONTRATOS

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Documento con el diseño de Alto Nivel de los servicios de Seguridad a los cuales se dara continuidad operativa 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	1% 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 los cuales se dara continuidad operativa 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	1% 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	1% 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	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Procedimientos de Operación del servicio • Servicios de Borrado Seguro de Información • Servicio de Gestión de Dominios	10 días hábiles posteriores a la integración de las mesas de trabajo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
• Servicio de Certificados Digitales SSL • Servicios de Ciberinteligencia (Ciberseguridad) • Servicios de Protección en Redes Inalámbricasy Seguridad en Dispositivos Móviles • Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA) • Servicios de Antivirus • Servicios de Prevención de Perdida de Información			
Metodología de implementación 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 posteriores a la integración de las mesas de trabajo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Partida 2.

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Procedimientos de Operación del servicio	10 días hábiles posteriores a la integración de las mesas de trabajo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
• Servicio de Análisis de Vulnerabilidades Estático • Servicio de Análisis de Vulnerabilidades Dinámico • Servicios de Análisis Forense • Servicio de Pruebas de Penetración			

Servicios del Centro de Operaciones de Seguridad (SOC)

Partida 1.

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Procesos de operación implementados: Requerimientos Cambios Configuraciones Incidentes Problemas Monitoreo	15 días naturales posteriores a la emisión del fallo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Matriz de Escalación Técnica y Organizacional	15 días naturales posteriores a la emisión del fallo	1% por cada día hábil 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 emisión del fallo	1% por cada día hábil 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	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

- **Deducciones**

En términos de los artículos 53 Bis de Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 97 de su Reglamento, en caso de incumplimiento parcial o deficiente en la prestación del servicio por causas

imputables al proveedor, El IMSS aplicará deducciones sobre el monto mensual facturado por pago del servicio de acuerdo con lo siguiente:

Durante la vigencia del contrato, al presentarte una falla, incidente, atención de requerimientos, ventana de mantenimiento, entre otras, y la causa raíz de estos eventos es atribuible a un tercero, no se aplicará una deducción al proveedor de SASI 2025 por el servicio relacionado, siempre y cuando pueda demostrar con pruebas concretas que el servicio en cuestión se brindó conforme a las especificaciones del anexo técnico y los términos y condiciones acordados.

El monto máximo de las deductivas, por ningún motivo podrán exceder del monto de la garantía de cumplimiento del contrato.

Conforme a lo anterior, en los casos en que las fallas, incidentes, atención de requerimientos, ventanas de mantenimiento, u otras eventualidades, sean atribuibles a la prestación de los servicios de seguridad por parte del Proveedor, se aplicarán deducciones según los siguientes rubros:

Disponibilidad

Partida 1.

La disponibilidad se define como el porcentaje de tiempo durante el cual el sistema que proporciona el servicio de seguridad de SASI 2025, o cualquier componente de este, cumple con su función designada. En otras palabras, la disponibilidad representa la proporción de tiempo en la que el sistema opera según su propósito previsto, en comparación con el tiempo en el que debería haber estado operativo.

Las mediciones de disponibilidad deben ser realizadas por el Proveedor de SASI 2025, utilizando las herramientas correspondientes de monitoreo del servicio y gestión de incidentes, con el objetivo de obtener mediciones precisas de los periodos operativos y no operativos, así como de sus causas.

Estas mediciones de disponibilidad deben llevarse a cabo desde el inicio del período operativo de los servicios de seguridad "SASI 2025", para todos los módulos o posiciones de servicio contratados.

El LICITANTE se compromete a garantizar la disponibilidad con base en los siguientes factores:

- Se incluyen todos los componentes WAN, LAN, dispositivos de seguridad y otros dispositivos que respaldan el servicio de seguridad, así como su configuración lógica equivalente.

El método de medición se basará en una correlación de los datos recopilados cada 5 minutos por el sistema de monitoreo, con los períodos de indisponibilidad identificados en los incidentes abiertos en el sistema de gestión de incidencias del proveedor de SASI 2025. Se excluirán los períodos de indisponibilidad cuya responsabilidad no sea atribuible al Proveedor de SASI 2025. El procedimiento de medición se describe de la siguiente manera:

- Se calcula con base en un período mensual de 30 días.
- Se calcula a partir del inicio de la falla.
- Se considera que está indisponible cuando el protocolo de la interfaz está inactivo (Down) o cuando hay una caída de tráfico atribuible a la infraestructura del proveedor.
- Solo se calcula con base en base fallas atribuibles al proveedor.

Disponibilidad por sitio y por posición de servicio

Las interrupciones causadas por fallos de energía que sean responsabilidad del Instituto no se considerarán en el cálculo de la disponibilidad.

$$\text{Disponibilidad_del_Servicio} = \left[\frac{\text{Tiempo_Total} - (\text{Tiempo_Indisponible} - \text{Tiempo_Instituto})}{\text{Tiempo_Total}} \right] X100$$

Dónde:
Tiempo Total: Tiempo total de disponibilidad para el mes de medición.

ANEXOS
DIVISIÓN DE CONTRATOS

Tiempo Indisponible: Tiempo indisponible según plataforma de monitoreo.
Tiempo Instituto: Tiempos atribuibles al Instituto extraídos del sistema de administración de incidentes.

Objetivos de la 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%

Deducción por incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Cuando no se cumplan con los objetivos de servicio, para los diferentes niveles de disponibilidad, conforme al esquema de medición propuesto	% de 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

Tiempo de detección y solución de fallas

Partida 1.

La métrica de tiempo de solución a fallas es independiente de la métrica de disponibilidad, ya que se refiere al lapso en el cual uno o varios servicios serán restituidos a su funcionamiento normal luego de presentarse una falla. Las mediciones del Tiempo de Solución de Fallas deberán ser llevadas a cabo por el LICITANTE , utilizando su herramienta correspondiente de gestión y monitoreo del servicio. El LICITANTE deberá efectuar dichas mediciones de manera mensual, tomando en cuenta el promedio del tiempo requerido para resolver cada tipo de severidad. La metodología por emplear, así como las herramientas y los responsables de las mediciones, serán definidos en las mesas de trabajo.

El Tiempo de Solución a Fallas se clasifica en cuatro categorías, según la severidad, causa e impacto de estas:

Severidad Crítica: Denota un incidente de alto impacto debido al riesgo que implica. Este tipo de incidente tiene el potencial de causar afectaciones y daños significativos en los activos y servicios del cliente. Puede incluir eventos como la interrupción total del servicio, la pérdida completa del sistema de comunicaciones y/o seguridad, la degradación de los recursos del Instituto, o la identificación de vulnerabilidades en la infraestructura protegida. Se considera una alarma significativa en el sistema de gestión cuando persiste durante más de 10 minutos.

Severidad Alta: Describe un incidente significativo en el que se experimenta una degradación, aunque no necesariamente una interrupción en los servicios e infraestructura protegidos por dispositivos de alta disponibilidad o seguridad. Este tipo de incidente se manifiesta a través de bloqueos o un rendimiento deficiente al intentar acceder a ciertos servicios de red que dependen de los dispositivos de comunicación y/o seguridad. También puede implicar la pérdida parcial de funcionalidades en el equipo de comunicaciones y/o seguridad. Estos eventos causan una degradación en el servicio sin llegar a provocar su interrupción completa.

Severidad Media: Este tipo de incidente se considera menor ya que no tiene un impacto significativo en los servicios o infraestructura protegidos por los dispositivos de seguridad. Por lo general, involucra problemas como fallas en la visualización de registros de actividad o dificultades en la comunicación entre servicios internos del Instituto y un grupo reducido de usuarios. Estos eventos suelen resultar en interrupciones en la disponibilidad del servicio durante períodos de tiempo cortos, generalmente inferiores a 10 minutos.

Severidad Baja: Estos casos se clasifican como preventivos con el propósito de mejorar u optimizar cualquier servicio de seguridad. La atención de estos casos de baja severidad deberá ser llevada a cabo por ingenieros del proveedor de servicios en el sitio, con la colaboración del fabricante a través de un centro de asistencia técnica personalizada. El tiempo de resolución de este tipo de incidencias será acordado entre el Instituto y el proveedor al momento de presentarse el caso.

La severidad de un incidente es determinada por el Instituto . Se establece la severidad, así como su nivel de escalación, en función de la operación y la criticidad de un servicio, basándose en los siguientes criterios:

SEVERIDAD	AFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
Critica	Una falla de alto impacto representa un problema crítico que impide por completo la operación de un servicio vital, el cual es fundamental para respaldar una función empresarial del Instituto a nivel nacional.	10 minutos posteriores a la detección de la falla	2 horas posteriores al registro y notificación de la falla
Alta	Se trata de un fallo que ocasiona una degradación en el servicio, impidiendo su correcto funcionamiento. Este servicio es crucial para respaldar una función de negocio dentro del Instituto, aunque su impacto se limita a nivel local y no afecta a escala nacional.	20 minutos posterior a la detección de la falla	4 horas posterior al registro y notificación de la falla
Media	Se trata de una falla menor que afecta la operación de un servicio específico del Instituto, impactando a un reducido grupo de usuarios.	120 minutos posterior a la detección de la falla	48 horas posterior al registro y notificación de la falla
Baja	Se consideran casos preventivos que buscan mejorar u optimizar cualquier servicio de seguridad. Estos casos tienen un impacto mínimo en la operación del negocio y pueden ser atendidos o resueltos según un calendario establecido.	5 días hábiles posterior a la detección de la falla	Se establecerá un acuerdo entre el Instituto y el Proveedor de SASI 2025, conforme a las mesas de trabajo que se establezcan con este fin.

Deducción por incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de registro y notificación conforme al nivel de severidad critica	10 minutos posteriores al registro y notificación de la falla	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

ANEXOS
DIVISIÓN DE CONTRATOS

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de solución conforme al nivel de severidad critica	2 horas posteriores al registro y notificación de la falla	Hora	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad alta	20 minutos posteriores al registro y notificación de la falla	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad alta	4 horas posteriores a la registro y notificación de la falla	Hora	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad media	120 minutos posteriores al registro y notificación de la falla	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad media	48 horas posteriores al registro y notificación de la falla	Hora	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad baja	5 días hábiles posteriores al registro y notificación de la falla	Día	0.2% por cada día hábil de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad baja	Se define entre el Instituto y el Proveedor de SASI 2025 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

Partida 1.

Un incidente es aquel evento, que, de materializarse, podrían comprometer la seguridad de la red y los activos de información que componen las misma, así como las aplicaciones que dan tratamientos a información de usuarios externos e internos.

De igual manera una actividad sospechosa es aquel evento que, de materializarse, podría comprometer la seguridad de la información, convirtiéndose en un incidente de seguridad.

Los incidentes se definen como la constatación de una violación a las políticas de seguridad informática o al uso aceptable de prácticas y políticas de seguridad estandarizadas, representando una evidencia clara de la vulneración de la confidencialidad, integridad y disponibilidad de la información, misma que puede presentarse por un factor externo, como por la ejecución incorrecta a través de un recurso interno (SOC).

Las métricas de tiempo relacionadas con el registro y la notificación se refieren al periodo en el que el proveedor SASI 2025 informa al Instituto sobre la confirmación de un incidente de seguridad. Estas métricas deben cumplirse según la prioridad establecida a partir de la apertura de un registro vinculado a un incidente de

seguridad. Respecto al tiempo de contención, se espera que el Proveedor de SASI 2025 detenga y aísle el incidente tras su detección, de acuerdo con los tiempos definidos para cada nivel de prioridad.

Todas estas mediciones deberán ser llevadas a cabo por el proveedor de SASI 2025 utilizando las herramientas correspondientes de gestión y monitoreo del servicio. Además, el proveedor deberá realizar estas mediciones de manera mensual, conforme al nivel de servicio establecido para cada tipo de métrica y/o prioridad.

Objetivos de la métrica

SEVERIDAD	AFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
Critica	Se refiere a un incidente de gran impacto que interrumpe por completo la operación de un servicio vital para una función empresarial del Instituto a nivel nacional.	10 minutos posteriores a la detección del incidente	60 minutos posteriores al registro y notificación del incidente
Alta	Se refiere a un incidente que ha provocado una degradación en el servicio, impidiendo su correcta operación. Este servicio es crucial para respaldar una función de negocio dentro del Instituto, aunque es importante destacar que su impacto se limita a nivel local y no afecta a nivel nacional.	20 minutos posterior a la detección del incidente	240 minutos posteriores al registro y notificación del incidente
Media	Se trata de un incidente menor que afecta a un pequeño grupo de usuarios del Instituto, impidiendo temporalmente el normal funcionamiento de un servicio.	30 minutos posterior a la detección del incidente	60 minutos posteriores al registro y notificación del incidente
Baja	Estos casos se consideran preventivos con el objetivo de mejorar u optimizar cualquier servicio de seguridad. Tienen un impacto mínimo en la operación del negocio y su atención y/o solución puede ser programada con antelación.	60 minutos posterior a la detección del incidente	2,880 minutos posteriores al registro y notificación del incidente

Deducción por incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de registro y notificación	10 minutos posteriores al	Minuto	0.5% por cada minuto de atraso en	Valor unitario de la facturación mensual del

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
conforme al nivel de severidad critica	registro y notificación del incidente		el registro y notificación	servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad critica	60 minutos posteriores al registro y notificación del incidente	Minuto	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad alta	20 minutos posteriores al registro y notificación del incidente	Minuto	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad alta	240 minutos posteriores al registro y notificación del incidente	Minuto	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad media	30 minutos posteriores al registro y notificación del incidente	Minuto	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad media	1,440 minutos posteriores al registro y notificación del incidente	Minuto	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad baja	60 minutos posteriores al registro y notificación del incidente	Minuto	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad baja	2,880 minutos posteriores al registro y notificación del incidente	Minuto	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Solicitudes de requerimientos y cambios

Partida 1

Consiste en el tiempo requerido por el Proveedor de SASI para llevar a cabo altas, cambios o bajas en la infraestructura del servicio de seguridad. Estas acciones se basarán en un conjunto de configuraciones preestablecidas, definidas durante las correspondientes mesas de trabajo. Dichas configuraciones serán diseñadas para satisfacer las necesidades de conectividad y flujos de información de las aplicaciones del Instituto. Se reconoce que la complejidad en la atención de estas tareas es mínima, dado que se cuenta con experiencia y conocimiento previo sobre las mismas configuraciones utilizadas en los módulos de los servicios de seguridad actualmente en funcionamiento.

Objetivos de la métrica

PRIORIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE EJECUCIÓN
Alta	Solicitud generada por el Instituto para abordar necesidades operativas urgentes.	10 minutos posteriores a la solicitud formal por parte del Instituto	60 minutos posteriores al registro realizado por el Instituto

PRIORIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE EJECUCIÓN
Media	Solicitud emitida por el Instituto para atender necesidades operativas habituales.	30 minutos posteriores a la solicitud formal por parte del Instituto	480 minutos posteriores al registro realizado por el Instituto
Baja	Solicitud generada por el Instituto para abordar necesidades operativas planificadas.	60 minutos posteriores a la solicitud formal por parte del Instituto	1,440 minutos posteriores al registro realizado por el Instituto

Cambios

Cualquier modificación realizada por el Proveedor, sin la autorización del Instituto, que resulte en una falla en los servicios de seguridad, será considerada como un incidente de seguridad. Este incidente será clasificado según las afectaciones o riesgos que haya generado.

PRIORIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE EJECUCIÓN
Emergente	Se requerirán cambios inmediatos en la infraestructura de la red en caso de experimentar una pérdida repentina del servicio, fallo en cualquiera de los activos de infraestructura, o a solicitud expresa del Instituto.	1 hora posteriores a la solicitud formal por parte del Instituto	Conforme al plan de trabajo definido entre el Instituto y el Proveedor
Normal	Modificaciones necesarias para mejorar o restablecer un servicio o expandir un activo de infraestructura, que no están contempladas en el catálogo de cambios estándar, requieren un análisis y aprobación por parte del Instituto.	1 hora posteriores a la solicitud formal por parte del Instituto	Conforme al plan de trabajo definido entre el Instituto y el Proveedor
Estándar	Actualizaciones en los servicios y/o activos de infraestructura que se ejecutan de manera online y siguen un proceso establecido, constituyendo una solución aceptada para un conjunto específico de requerimientos.	1 hora posteriores a la solicitud formal por parte del Instituto	24 horas posterior al registro realizado por el Instituto

Deducción por incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de registro y notificación conforme al nivel de prioridad Alta	10 minutos posteriores al registro y notificación del requerimiento	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de ejecución conforme al nivel de prioridad Alta	60 minutos posteriores al registro y notificación del requerimiento	Minuto	0.5% por cada minuto de atraso en la ejecución del requerimiento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Media	30 minutos posteriores al registro y notificación del requerimiento	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Media	8 horas posteriores al registro y notificación del requerimiento	Hora	0.5% por cada hora o fracción de atraso en la ejecución del requerimiento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Baja	60 minutos posteriores al registro y notificación del requerimiento	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Baja	24 horas posteriores al registro y notificación del requerimiento	Hora	0.5% por cada hora o fracción de atraso en la ejecución del requerimiento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Cambios

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de registro y notificación conforme al nivel de prioridad Emergente	60 minutos posteriores al registro y notificación del cambio	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de ejecución conforme al nivel de prioridad Emergente	Conforme al plan de trabajo definido entre el Instituto y el Proveedor	Hora	1% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Normal	60 minutos posteriores al registro y notificación del cambio	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Normal	Conforme al plan de trabajo definido entre el Instituto y el Proveedor	Hora	1% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de registro y notificación conforme al nivel de prioridad Estándar	60 minutos posteriores al registro y notificación del cambio	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Estándar	24 horas posteriores al registro y notificación del cambio	Hora	1% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Servicios de Seguridad – Continuidad Operativa

Partida 1.

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Reportes Técnicos de los activos de infraestructura que contemplen: ▪ 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 posteriores al cumplimiento del mes vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Servicios de Seguridad – Verificación/Calidad

Partida 1.

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Reportes Técnicos de los activos de infraestructura que contemplen: ▪ Disponibilidad ▪ Controles de Cambios ▪ Requerimientos ▪ Incidentes/Falla	5 días hábiles siguientes al vencimiento del mes.	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
▪ Actividad Sospechosa ▪ Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)				
Servicios de Borrado Seguro de Información: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado.	5 días hábiles siguientes al vencimiento del mes.	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicio de Gestión de Dominios: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos.	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicio de Certificados Digitales SSL: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los certificados que se hayan renovado o adquiridos (incluyendo archivo electrónico compreso con la llave publica relacionado con los requerimientos)	1 día hábil posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Servicios de Ciberinteligencia: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de amenazas y ataques potenciales a los que se encuentra expuesto el Instituto que incluya: Situación general del evento, hallazgos detectados, mecanismos de inteligencia accionable, táctica u operativa recomendados para prevención y/o contención	1 día hábil posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos Móviles: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las politicas, configuraciones o reportes solicitados por el Instituto	1 día hábil posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA): Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las politicas, configuraciones o reportes solicitados por el Instituto	5 días hábiles posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Antivirus: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las politicas, configuraciones o reportes solicitados por el Instituto.	1 día hábil posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Prevención de Pérdida de Información:	1 día hábil posterior a la solicitud generada	Día	1% por cada día hábil de atraso en la entrega	Valor unitario de la facturación mensual del servicio

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las politicas, configuraciones o reportes solicitados por el Instituto.	por parte del Instituto		de los reportes 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 posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del plan de trabajo	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Sistema de Gestión de Seguridad de la Información: Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora del Sistemas De Gestión de Seguridad de la Información (SGSI)	Conforme a la fecha estipulada en el plan de trabajo acordado entre el Instituto y el Proveedor	Día	1% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, por evento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Gestión del Cambio en Seguridad de la Información: Plan de Trabajo de implementación y operación de los servicios conforme al alcance definido en las mesas de trabajo	10 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del plan de trabajo	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Gestión del Cambio en Seguridad de la Información: Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora de la Gestión del Cambio en Seguridad de la Información	Conforme a la fecha estipulada en el plan de trabajo acordado entre el Instituto y el Proveedor	Día	1% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, por evento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Partida 2.

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Servicio de Análisis de Vulnerabilidades Estático Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada pieza de software (código) escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis	7 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicio de Análisis de Vulnerabilidades Dinámico Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas	7 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
para el proceso de análisis				
Servicios de Pruebas 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	10 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Análisis Forense: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de infraestructura verificados	15 días hábiles posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Servicios del Centro de Operaciones de Seguridad (SOC)

Cualquier modificación realizada por el SOC, sin autorización previa del Instituto, ya sea que cause o no una falla en los servicios de seguridad, se considerará como un incidente de seguridad. Este incidente será clasificado según las afectaciones o riesgos que pueda haber ocasionado.

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	5 días hábiles siguientes al término 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 siguientes al término 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 siguientes al término 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 siguientes al término 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 siguientes al término del mes vencido.	Día	1% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte de las evaluaciones operativas a los servicios de seguridad implementados	5 días hábiles posteriores al cumplimiento del trimestre vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte que integre el calendario de actualizaciones de versionamiento en software de cada servicio implementados	5 días hábiles posteriores al cumplimiento del trimestre vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Creación de cuentas de acceso en las consolas de administración de los servicios de seguridad	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada	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	FÓRMULA DE CÁLCULO
	solicitud generada por el Instituto			
Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto	Día	1% por cada día hábil de atraso en la entrega de las cuentas de acceso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Actualización de la matriz de escalación	5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad	Día	1% por cada día hábil de atraso en la entrega de la matriz de escalación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad	5 días hábiles posteriores a la ejecución de la ventana mantenimiento	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de las configuraciones de las soluciones de seguridad	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de los incidentes presentados en las soluciones de seguridad	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de los requerimientos registrados en la mesa de servicios	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y su diagrama de	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
interrelación conforme fueron registrados en la CMDB				
Diagramas de Arquitectura de las soluciones de seguridad	2 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tablero de Estadísticas de Servicios de Seguridad (Portal Único)	10 días hábiles posteriores al término de la habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo	Día	1% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, por evento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

11. Mecanismos requeridos al proveedor para responder por defectos o vicios ocultos de los bienes o de la calidad de los servicios.

No aplica

12. Garantías de anticipos y cumplimiento.

El proveedor, para garantizar el cumplimiento de todas y cada una de las obligaciones estipuladas en el contrato adjudicado, de conformidad con lo establecido en el numeral 4.30.1 de las POBALINES, deberá presentar copia simple de la fianza expedida por afianzadora debidamente constituida en términos de la Ley de Instituciones de Seguros y de Fianzas, por un importe equivalente al 10% (diez por ciento) del monto máximo del contrato, sin incluir el impuesto al Valor Agregado, a favor del Instituto Mexicano del Seguro Social, la cual será divisible.

La vigencia de la fianza deberá quedar abierta durante la vigencia del contrato para permitir que cumpla con su objetivo.

El proveedor en término de lo dispuesto en el artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, deberá entregar al INSTITUTO MEXICANO DEL SEGURO SOCIAL dentro de los 10 (diez) días naturales siguientes a la firma del contrato el original de la fianza a la División de Contratos, ubicada en Calle Durango número 291, 10° piso, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700 Ciudad de México.

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

a) Plazo para notificar al proveedor.

La garantía de cumplimiento del contrato deberá presentarse en el plazo o fecha previstos en la convocatoria a la licitación; en su defecto, a más tardar dentro de los diez días naturales siguientes a la firma del contrato.

ANEXOS
DIVISIÓN DE CONTRATOS

b) La existencia de consumibles y refacciones, en su caso.

No aplica

c) Plazo y condiciones de canje o devolución del bien.

No aplica

d) Caducidad de los bienes.

No aplica

e) Centros de servicio (domicilios y horarios) y reporte técnico.

No aplica

f) Periodo de garantía.

Durante la vigencia del contrato

g) Tiempos máximos de reparación o atención de fallas.

Conforme lo establecido en el documento de términos y condiciones, en su numeral 10.Penas convencionales y deductivas.

h) Garantía de mano de obra y/o partes.

No aplica

i) Mantenimientos correctivos y/o preventivos.

No aplica

j) En su caso, si se requiere capacitación, solicitar programa para la misma.

No aplica

k) Porcentaje a requerir por concepto de garantía de cumplimiento.

Por un importe equivalente al 10% (diez por ciento) del monto máximo del contrato, sin considerar el impuesto al valor agregado, a favor del Instituto.

13. Forma de pago.

El servicio descrito en el Anexo Técnico está modelado con base en un esquema de pago unitario mensual conforme a las entregas programadas, el cual se realizará en moneda nacional y conforme al siguiente esquema:

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

14. Mecanismos de comprobación, supervisión y verificación de los bienes o de los servicios contratados.

Para este fin, se llevarán a cabo reuniones mensuales en las que se revisará la operación del licitante adjudicado, comparándola con los indicadores de niveles de servicio acordados. Esta evaluación se plasmará en un documento denominado 'Acta Administrativa de Entrega-Recepción Mensual de los Servicio Administrado de Seguridad de la Información SASI 2025. La periodicidad de esta acta será mensual desde el inicio de la prestación del servicio y se realizará dentro de los 5 días hábiles posteriores al cierre de cada mes.

En consecuencia, el proveedor reconoce expresamente que el servicio no será considerado como aceptado o recibido por parte del Instituto hasta que se cumpla conforme a lo establecido en los párrafos anteriores.

Todas las actas mencionadas en este apartado deberán contar con la firma de conformidad del Administrador del Contrato del IMSS y ser elaboradas en cuatro tantos originales: uno para el licitante adjudicado, otro para el Administrador del Contrato, un tercero para el expediente de la Coordinación de Telecomunicaciones y Seguridad de la Información, y el último para la División de Trámite de Erogaciones.

15. Anticipo.

El instituto no otorgará anticipos.

16. Aviso de privacidad y medidas de seguridad para el manejo de la información para bienes o servicios de TIC.

No aplica

17. Seguro de Responsabilidad Civil.

No aplica

18. Dictámenes de protección civil emitidos por las autoridades competentes en la materia.

No aplica

19. Confidencialidad

Tanto el Instituto como el proveedor acuerdan considerar como información confidencial todo material, impreso o electrónico, que contenga datos, grabaciones, programas de cómputo o cualquier otro contenido vinculado a información jurídica, operativa, técnica, financiera, análisis, registros, documentos, especificaciones, productos, informes, dictámenes o desarrollos, tanto aquellos a los que tenga acceso como los proporcionados durante la prestación del servicio. Asimismo, se considerará como confidencial toda la información facilitada por el Instituto Mexicano del Seguro Social para la ejecución del servicio y que sea exclusiva propiedad del Instituto Mexicano del Seguro Social.

El proveedor reconoce que está terminantemente prohibida la divulgación total o parcial de esta información a su favor o a terceros ajenos a la relación contractual, por cualquier medio disponible, incluyendo, de manera enunciativa mas no limitativa, vía oral, impresa, electrónica, magnética, óptica, o cualquier otro medio, conforme a los plazos establecidos en la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables en la materia."

El proveedor reconoce y acepta la prohibición mencionada en el párrafo anterior, comprendiendo que está absolutamente prohibido divulgar la información del Instituto con fines de lucro, comerciales, académicos, educativos u otros ajenos al propósito de la presente contratación. En consecuencia, el proveedor asume la responsabilidad del uso y cuidado de la información.

ANEXOS
DIVISIÓN DE CONTRATOS

En virtud de lo anterior, el proveedor se compromete a mantener una estricta confidencialidad sobre la información a la que acceda, asegurando que cada miembro del personal asignado para el desarrollo y operación del proyecto respete el manejo adecuado de dicha información.

Considerar como confidencial toda la información a la que tenga acceso el personal designado para prestar los servicios objeto de esta contratación. El proveedor se compromete a garantizar que dicho personal no copie ni respalde información del Instituto Mexicano del Seguro Social en ningún equipo sin la previa autorización por escrito por parte del Instituto.

Garantizar que el acceso a la información del Instituto Mexicano del Seguro Social esté restringido únicamente al personal autorizado por el Instituto. El incumplimiento de estas condiciones será considerado como una violación de la confidencialidad y protección de datos personales.

Además, cualquier persona que tenga acceso a esta información deberá ser informada y comprometida a cumplir con lo establecido en el Anexo Técnico de esta contratación

Es importante destacar que la información proporcionada por el Instituto al proveedor para la prestación del servicio no otorgará al proveedor titularidad o derechos de autor, ni de ninguna otra índole.

El proveedor será responsable en el caso de que se violen derechos de propiedad industrial, patentes o derechos de autor, respecto al software y/o hardware utilizados para brindar el servicio, dejando en todo momento a salvo a el Instituto.

20. Propiedad intelectual

Durante el período de garantía de las licencias, el proveedor se compromete a eximir al Instituto de cualquier responsabilidad de índole civil, mercantil, penal o administrativa que pudiera surgir como resultado de la violación de derechos de autor, patentes, marcas u otros derechos de propiedad industrial o intelectual, tanto a nivel nacional como internacional. Esta exención de responsabilidad abarca cualquier reclamo, demanda, acción legal o procedimiento que pueda surgir contra el Instituto como consecuencia de dicha infracción. Además, el proveedor se compromete a asumir todos los costos, gastos, multas o indemnizaciones que puedan derivarse de tales reclamaciones, eximiendo al Instituto de cualquier carga económica asociada a las mismas.

21. Tipo de abastecimiento.

El tipo de abastecimiento será mediante dos partidas.

22. Modalidad del contrato

Contrato de modalidad abierta.

23. Representante del Área Técnica y Auxiliar del Administrador del Contrato

El Ing. Abraham Gutiérrez Castillo, Titular de la División de Seguridad Informática Física, fungirá como responsable del "Área Técnica", así como "Auxiliar del Administrador del Contrato"

24. Administración de la Contratación

El Ing. Javier Cortes López, Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información, fungirá como "Administrador del Contrato"

25. Representante del Área Requirente de la Contratación

El Ing. Javier Cortes López, Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información, fungirá como "ÁREA REQUIRENTE"

26. Firmas de elaboración, revisión y aprobación

Elaboró/Revisó	Cargo	Firma	Fecha
Ing. Abraham Gutiérrez Castillo	Titular de la División de Seguridad Informática Física		01/04/2025

Aprobó	Cargo	Firma	Fecha
Ing. Javier Cortes López	Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información		01/04/2025

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

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** **050GYR019N15725-001-00**

ANEXO 3 (TRES)

"PROPUESTA TÉCNICA Y ECONÓMICA, DE "EL PROVEEDOR", OFICIO DE NOTIFICACIÓN DE ADJUDICACIÓN Y OFICIO NÚMERO 09 53 84 61 1CFE/2025/007676"

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

Propuesta Técnica
Términos y Condiciones.

Operbes, S.A. de C.V. participa en la Partida 1

ANEXOS
DIVISIÓN DE CONTRATOS

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

Contenido

1. Objetivo del documento 3
2. Vigencia de la contratación y ejercicio presupuestal al que corresponda. 3
3. Plazo de entrega del bien, arrendamiento o servicio. 3
El plazo será a partir del 01 de enero de 2025 y hasta el 31 de diciembre de 2025. En caso de que el procedimiento de contratación exceda el 01 de enero de 2025, el plazo será a partir del día hábil sigueinte a la notificación del fallo y hasta el 31 de diciembre de 2025. 3
4. Criterio de evaluación. 3
5. Licencias, permisos, registros, certificados o autorizaciones. 4
6. Folletos, catálogos, fotografías, manuales entre otros. 8
7. Visitas a las instalaciones institucionales. 8
8. Lugar de entrega. 8
9. Visitas a las instalaciones del licitante. 8
10. Penas convencionales y deductivas. 8
11. Mecanismos requeridos al proveedor para responder por defectos o vicios ocultos de los bienes o de la calidad de los servicios. 26
12. Garantías de anticipos y cumplimiento. 26
a) Plazo para notificar al proveedor. 26
b) La existencia de consumibles y refacciones, en su caso. 26
c) Plazo y condiciones de canje o devolución del bien. 26
d) Caducidad de los bienes. 26
e) Centros de servicio (domicilios y horarios) y reporte técnico. 26
f) Periodo de garantía. 27
g) Tiempos máximos de reparación o atención de fallas. 27
h) Garantía de mano de obra y/o partes. 27
i) Mantenimientos correctivos y/o preventivos. 27
j) En su caso, si se requiere capacitación, solicitar programa para la misma. 27
k) Porcentaje a requerir por concepto de garantía de cumplimiento. 27
13. Forma de pago. 27
14. Mecanismos de comprobación, supervisión y verificación de los bienes o de los servicios contratados. 27
15. Anticipo. 28
16. Aviso de privacidad y medidas de seguridad para el manejo de la información para bienes o servicios de TIC. 28
17. Seguro de Responsabilidad Civil. 28
18. Dictámenes de protección civil emitidos por las autoridades competentes en la materia. 28
19. Confidencialidad 28
20. Propiedad intelectual 29
21. Tipo de abastecimiento. 29
22. Modalidad del contrato 29
23. Área Requirente y Técnica 30
24. Administrador del contrato y responsable de la supervisión del mismo 30
25. Firmas de elaboración, revisión y aprobación **¡Error! Marcador no definido.**

ANEXOS
DIVISIÓN DE CONTRATOS

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

1. **Objetivo del documento**

Operbes S.A. de C.V. tomó en consideración que que el objetivo del presente documento es definir las necesidades y condiciones para la entrega de los "Servicios Administrados de Seguridad Informática 2025.

2. **Vigencia de la contratación y ejercicio presupuestal al que corresponda.**

Operbes S.A. de C.V. tomó en consideración que la vigencia contractual será a partir del 01 de enero de 2025 y hasta el 31 de diciembre de 2025. Operbes S.A. de C.V. tomó en consideración que en caso de que el procedimiento de contratación exceda el 01 de enero de 2025, la vigencia contractual será a partir del día hábil siguiente a la notificación del fallo y hasta el 31 de diciembre de 2025.

3. **Plazo de entrega del bien, arrendamiento o servicio.**

Operbes S.A. de C.V. tomó en consideración que el plazo será a partir del 01 de enero de 2025 y hasta el 31 de diciembre de 2025. En caso de que el procedimiento de contratación exceda el 01 de enero de 2025, el plazo será a partir del día hábil sigueinte a la notificación del fallo y hasta el 31 de diciembre de 2025.

4. **Criterio de evaluación.**

Operbes S.A. de C.V. tomó en consideración que la evaluación de las proposiciones podrá llevarse a cabo utilizando el criterio de puntos y porcentajes, centrándose exclusivamente en los requisitos para la prestación del servicio establecidos en el Anexo Técnico, así como en los Apendices A y B. Esto garantizará el cumplimiento satisfactorio de las respectivas obligaciones.

Operbes S.A. de C.V. tomó en consideración que bajo este enfoque, la adjudicación se otorgará al licitante que haya obtenido el mayor puntaje en su propuesta técnica y económica. En caso de situaciones no contempladas, se aplicarán los **"LINEAMIENTOS PARA LA APLICACIÓN DEL CRITERIO DE EVALUACIÓN DE PROPOSICIONES A TRAVÉS DEL MECANISMO DE PUNTOS O PORCENTAJES EN LOS PROCEDIMIENTOS DE CONTRATACIÓN",** publicados en el Diario Oficial de la Federación.

Operbes S.A. de C.V. tomó en consideración que el puntaje más alto, equivalente a 40 puntos, se asignará a la propuesta económica más baja. Para calcular el valor de las propuestas económicas superiores a la más baja, se utilizará la siguiente fórmula:

PPE = MPemb x 40 / MPi.

Dónde:

PPE = Puntuación o unidades porcentuales que corresponde a la Propuesta Económica
MPemb = Monto de la Propuesta Económica más baja
MPi = Monto de la i-ésima Propuesta Económica.

Operbes S.A. de C.V. tomó en consideración que se aceptarán las ofertas que cumplan con los requerimientos establecidos y cubran las características técnicas establecidas en el Anexo Técnico.

Operbes S.A. de C.V. tomó en consideración que la evaluación por el mecanismo de puntos o porcentajes consta de 100 puntos, de los cuales 40 puntos corresponden a la propuesta económica considerando el monto total de la propuesta conforme al formato de propuesta económica.

ANEXOS
DIVISIÓN DE CONTRATOS

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

Operbes S.A. de C.V. tomó en consideración que los 60 puntos restantes corresponden a la evaluación técnica, que consiste en la suma de la puntuación de los siguientes rubros, con sus respectivos apartados:

NÚMERO DE RUBRO	RUBRO	PUNTUACIÓN A OTORGAR
I	CAPACIDAD DEL **LICITANTE**	PUNTOS
II	EXPERIENCIA Y ESPECIALIDAD DEL **LICITANTE**	PUNTOS
III	PROPUESTA DE TRABAJO	PUNTOS
IV	CUMPLIMIENTO DE CONTRATOS	PUNTOS
TOTAL		**60 PUNTOS**

Operbes S.A. de C.V. tomó en consideración que la puntuación o unidades porcentuales para obtener en la propuesta técnica para ser considerada solvente y, por tanto, no ser desechada, será de cuando menos 45 de los 60 máximos que se pueden obtener en su evaluación, **conforme a lo señalado en el "Apéndice C - Matriz de Puntos o Porcentajes, Partida 1"**, así como en el **"Apendice D - Matriz de Puntos o Porcentajes, Partida 2".**

Operbes S.A. de C.V. tomó en consideración que la omisión total o parcial en la presentación de alguno de los rubros a evaluar **NO** será motivo de desechamiento. No obstante lo anterior, en tal caso el Instituto podrá abstenerse de asignar puntos en el rubro correspondiente.

5. Licencias, permisos, registros, certificados o autorizaciones.

Operbes S.A. de C.V. a continuacion incluye en su propuesta las sigueintes certificaciones vigentes y emitidas a nombre de Operbes S.A. de C.V.:

Normas Internacionales.

- Certificado ISO/IEC27001:2022
- Certificado ISO/IEC20000-1:2018

Vigentes y emitidas a nombre de Operbes S.A. de C.V.

ANEXOS
DIVISIÓN DE CONTRATOS

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

NYCE
Sistemas de Gestión

CERTIFICADO

Normalización y Certificación NYCE, S.C., organismo acreditado con el número 129/17, por la Entidad Mexicana de Acreditación A.C. (ema), certifica que el Sistema de Gestión de Seguridad de la Información de:

OPERBES, S.A. DE C.V.
MEXICO RED DE TELECOMUNICACIONES, S. DE R.L. DE C.V.
SERVICIOS TELUM, S.A. DE C.V

Monterrey No. 38, Piso 1, Col Napoles, C.P. 03810, Alcaldía Benito Juárez, CDMX, Mexico

Cumple de conformidad con los requisitos de la norma:

NMX-I-27001-NYCE-2015 / ISO/IEC 27001:2013

Con el siguiente alcance:

Todos los servicios y procesos mencionados a continuación son provistos por el área de SOC/CSIRT a través de los equipos de seguridad defensiva y ofensiva, mejor conocidos como Blue Team y Red Team, el portafolio y catálogo de Servicios soportados en los subsistemas operativos para la gestión de la calidad, gestión de servicios, gestión de la continuidad del negocio y la gestión de la seguridad de la información:•Procesos de gestión de riesgos, gestión de la capacidad, auditorías, no conformidades, acciones correctivas, seguridad de la red y mejora continua. •Servicios para la administración y gestión de cambios, soportado en los procesos de gestión de cambios, clasificación de requerimientos, gestión de solicitudes de servicio y cambios emergentes. •Servicios de respaldo de configuraciones, soportado en los procesos de respaldo, validación, gestión de activos de servicio y de la gestión de configuración. •Servicios de administración y gestión de incidentes, soportado en los procesos de gestión, identificación, clasificación y atención de incidentes. • Servicios de respuesta a incidentes de seguridad, soportado en los procesos de detección, notificación, análisis de incidentes de seguridad y ciber patrullaje. • Servicios de administración, gestión de eventos y actividad sospechosa, soportado en los procesos de monitoreo, investigación, dictamen de actividad sospechosa y blue team. • Servicios de administración y gestión de problemas, soportado en los procesos de atención, resolución de problemas y gestión del conocimiento. • Servicios de administración y gestión de vulnerabilidades, soportado en los procesos de clasificación y análisis de vulnerabilidades. • Servicios de monitoreo de disponibilidad, soportados en los procesos de gestión del servicio, gestión de la disponibilidad y gestión del desempeño. Servicios de difusión y alertas de seguridad, soportados en los procesos de evaluación de impacto de amenazas y elaboración de reportes de las alertas de seguridad• Servicios de auditorías y análisis de seguridad, soportado en los procesos de clasificación de los hallazgos del análisis de vulnerabilidades, explotación de vulnerabilidades y análisis e investigación forense digital. De acuerdo a la declaración de aplicabilidad con fecha 06 marzo 2022.

CERTIFICADO No. 2018CRI-003
Fecha de emisión: 2022-05-06
Vigente al: 2025-05-08
Certificado desde: 2013-05-09

Seguridad de la Información
ORGANIZACIÓN CERTIFICADA
ISO/IEC 27001

CUMPLIMIENTO NYCE REGISTRO

A Partner of IQNet

IAF ema
ACREDITADO 129/17

[redacted]

El presente certificado es propiedad de NYCE Sistemas de Gestión y deberá ser entregado de inmediato bajo solicitud expresa, de acuerdo con el "Reglamento de uso de la marca NYCE Sistemas de Gestión". Se puede consultar en línea la autenticidad del certificado en www.nyce.org.mx o contactando directamente al personal del departamento de NYCE Sistemas de Gestión. Cuando existan apendices adjuntos al certificado estos forman parte integral del mismo y deben ser leídos como un solo documento. El presente certificado es válido siempre que se cumpla de manera permanente con los requisitos bajo los cuales se obtuvo, sino suspensión o retiro notificado en tiempo por NYCE Sistemas de Gestión.

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: NOMBRE, FIRMA Y CARGO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

IQNet
THE INTERNATIONAL CERTIFICATION NETWORK

CERTIFICATE

Normalización y Certificación NYCE, S.C. has issued an IQNet recognized certificate that the organization:

OPERBES, S.A. DE C.V.
MEXICO RED DE TELECOMUNICACIONES, S. DE R.L. DE C.V.
SERVICIOS TELUM, S.A. DE C.V

Headquarter: Montecito No. 38, Piso 1, Col Nápoles, C.P. 03810, Benito Juárez, CDMX, México

has implemented and maintains a

Information Security Management System

for the following scope:

All the services and processes mentioned below are provided by the SOC / CSIRT area through the defensive and offensive security teams, better known as Blue Team and Red Team, the portfolio and catalog of Services supported in the operational subsystems for the quality management, service management, business continuity management and information security management: • Risk management processes, capacity management, audits, non-conformities, corrective actions, network security and continuous improvement. • Services for the administration and management of changes, supported in the processes of change management, requirements classification, service request management and emerging changes. • Configuration backup services, supported in the backup, validation, service asset management and configuration management processes. • Incident management and administration services, supported in the processes of management, identification, classification and attention to incidents • Security incident response services, supported in the detection, notification, analysis of security incidents and cyber patrol processes. • Administration services, management of events and suspicious activity, supported in the processes of monitoring, investigation, opinion of suspicious activity and blue team. • Administration and management services of problems, supported in the processes of attention, problem solving and knowledge management • Vulnerability management and administration services, supported in the vulnerability analysis and classification processes • Availability monitoring services, supported in the service management, availability management and performance management processes. Dissemination services and security alerts, supported in the processes for evaluating the impact of threats and preparing reports on security alerts. • Security auditing and analysis services, supported in the processes of classifying the findings of the vulnerability analysis, vulnerability exploitation and digital forensic analysis and investigation. According to the Applicability Statement dated March 04, 2022.

which fulfils the requirements of the following standard

ISO/IEC 27001:2013

Issued on: **2022-05-06**
Expires on: **2025-05-08**
First Issued: **2013-05-09**

This attestation is directly linked to the IQNet Partner's original certificate and shall not be used as a stand-alone document

Registration Number: **MX- 2018CRI-003**

IQNet [redacted] [redacted] NYCE Sistemas de Gestión

IQNet Partners*:
AENOR Spain AFNOR Certification France APCER Portugal CCC Cyprus CISQ Italy
CQC China CQM China CQS Czech Republic Cro Cert Croatia DQS Holding GmbH Germany EAGLE Certification Group USA
FCAV Brazil FONDONORMA Venezuela ICONTEC Colombia Inspecta Sertifiointi Oy Finland INTECO Costa Rica
IRAM Argentina JQA Japan KFQ Korea MIRTEC Greece MSZT Hungary Nemko AS Norway NSAI Ireland
NYCE-SIGE México PCBC Poland Quality Austria Austria RR Russia SII Israel SIQ Slovenia
SIRIM QAS International Malaysia SQS Switzerland SRAC Romania TEST St Petersburg Russia TSE Turkey YUQS Serbia

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: NOMBRE, FIRMA Y CARGO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

NYCE
Sistemas de Gestión

CERTIFICADO

Normalización y Certificación NYCE, S.C., organismo acreditado con el número 129/17, por la Entidad Mexicana de Acreditación A.C. (ema), certifica que el Sistema de Gestión de Servicios de

OPERBES, S.A. DE C.V.
MEXICO RED DE TELECOMUNICACIONES, S. A. DE R.L. DE C.V.
SERVICIOS TELUM, S.A. DE C.V.

Montecito No. 38, Piso 1, Col Nápoles, C.P. 03810, Alcaldía Benito Juárez, CDMX, México
Cumple de conformidad con los requisitos de la norma

NMX-I-20000-1-NYCE-2019 / ISO/IEC 20000-1:2018

Con el siguiente alcance:

Todos los servicios y procesos mencionados a continuación son provistos por el área de SOC/CSIRT a través de los equipos de seguridad defensiva y ofensiva, mejor conocidos como Blue Team y Red Team, el portafolio y catálogo de Servicios soportados en los subsistemas operativos para la gestión de la calidad, gestión de servicios, gestión de la continuidad del negocio y la gestión de la seguridad de la información:•Procesos de gestión de riesgos, gestión de la capacidad, auditorías, no conformidades, acciones correctivas, seguridad de la red y mejora continua. •Servicios para la administración y gestión de cambios, soportado en los procesos de gestión de cambios, clasificación de requerimientos, gestión de solicitudes de servicio y cambios emergentes. •Servicios de respaldo de configuraciones, soportado en los procesos de respaldo, validación, gestión de activos de servicio y de la gestión de configuración. •Servicios de administración y gestión de incidentes, soportado en los procesos de gestión, identificación, clasificación y atención de incidentes.• Servicios de respuesta a incidentes de seguridad, soportado en los procesos de detección, notificación, análisis de incidentes de seguridad y ciber patrullaje.• Servicios de administración, gestión de eventos y actividad sospechosa, soportado en los procesos de monitoreo, investigación, dictamen de actividad sospechosa y blue team.• Servicios de administración y gestión de problemas, soportado en los procesos de atención, resolución de problemas y gestión del conocimiento.• Servicios de administración y gestión de vulnerabilidades, soportado en los procesos de clasificación y análisis de vulnerabilidades.• Servicios de monitoreo de disponibilidad, soportados en los procesos de gestión del servicio, gestión de la disponibilidad y gestión del desempeño. Servicios de difusión y alertas de seguridad, soportados en los procesos de evaluación de impacto de amenazas y elaboración de reportes de las alertas de seguridad• Servicios de auditorías y análisis de seguridad, soportado en los procesos de clasificación de los hallazgos del análisis de vulnerabilidades, explotación de vulnerabilidades y análisis e investigación forense digital. De acuerdo a la declaración de aplicabilidad con fecha 04 marzo 2022.

[redacted]ADO No. 2018CRG-007
de emisión. 2022-05-06
Vigente al: 2025-05-08
cado desde: 2013-05-09

[redacted]

A Partner of IQNet

ema
ORGANISMO DE CERTIFICACIÓN
ACREDITADO 129/17

El presente certificado es propiedad de NYCE Sistemas de Gestión y deberá ser entregado de inmediato bajo solicitud expresa de acuerdo con el "Reglamento de uso de la marca NYCE Sistemas de Gestión". Se puede consultar en línea la autenticidad del certificado en www.sige.org.mx o contactando directamente al personal del departamento de NYCE Sistemas de Gestión. Cuando existan apéndices adjuntos al certificado, estos forman parte integral del mismo y deben ser leídos como un solo documento. El presente certificado es válido siempre que se cumpla de manera permanente con los requisitos bajo los cuales se otorgó, salvo suspensión o retiro notificado en tiempo por NYCE Sistemas de Gestión.

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: NOMBRE, FIRMA Y CARGO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

6. Folletos, catálogos, fotografías, manuales entre otros.

Los folletos, hojas de especificaciones, y demás documentación técnica, estarán integrados como parte de la propuesta de Operbes S.A. de C.V., misma que será verificada a través del dictamen técnico que se emita por parte del Área Técnica.

En caso de que los documentos referidos en el párrafo que antecede vengan en su idioma de origen y sea diferente al español, Operbes S.A. de C.V. incluirá una traducción al español. Operbes S.A. de C.V. tomó en consideración que no presentar la trraducción al español de los documentos que se encuentren en otro idioma será motivo de desechamiento de la propuesta, en cuyo caso no pasarña a la evaluación de puntos o procentajes.

Para dar cumplimiento con lo anterior Favor de referirse al APARTADO FOLLETOS y memoriua USB entregada como parte de la presente propuesta.

7. Visitas a las instalaciones institucionales.

Operbes S.A. de C.V. tomó en consideración que no aplica

8. Lugar de entrega.

Operbes S.A. de C.V. tomó en consideración que la entrega se realizará en las instalaciones del Instituto ubicadas en Avenida Paseo de la Reforma 476, Anexo de Telecomunicaciones Planta Alta, Colonia Juárez, Delegación Cuauhtémoc, Ciudad de México, C.P. 06600.

9. Visitas a las instalaciones del licitante.

Operbes S.A. de C.V. tomó en consideración que no aplica

10. Penas convencionales y deductivas.

- **Penas convencionales**

De conformidad con lo establecido en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como el 85 fracción V, 95 y 96 de su Reglamento, numeral 5.5.8. de las Políticas, Bases y Lineamientos del IMSS, el administrador del contrato llevará a cabo el cálculo y la aplicación de las penas convencionales, según lo estipulado en contrato, notificando a Operbes S.A. de C.V. para proceder con el pago correspondiente.

Operbes S.A. de C.V. estará sujeto a penas convencionales por cada día hábil de retraso en el cumplimiento de las fechas pactadas de entrega o de la prestación del servicio.

El incumplimiento en la prestación del servicio será determinado por el Administrador del Cumplimiento del contrato, quien calculará y notificará por escrito el monto de la pena convencional a Operbes S.A. de C.V.

El monto máximo de las penas convencionales por atraso no podrá exceder del monto de la garantía de cumplimiento del contrato y se aplicará sobre el monto total sin incluir el Impuesto al Valor Agregado ni el Impuesto Especial sobre Producción y Servicios.

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

Operbes S.A. de C.V. tomó en consideración que en ningún caso las penas convencionales podrán negociarse en especie.

Servicios de Habilitación, Operación y Transición
Partida 1 y 2.

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Plan de trabajo detallado de los servicios del proyecto	15 días hábiles posteriores a la emisión del fallo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Documento Compromiso de suscripción de OLAs	15 días hábiles posteriores a la emisión del fallo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Matriz de Escalación	15 días hábiles posteriores a la emisión del fallo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Se proporcionará un documento por parte de Operbes S.A. de C.V., firmado por su representante legal, en el cual se declaren las habilidades, competencias y capacidades necesarias para respaldar la prestación de los servicios requeridos.	15 días hábiles posteriores a la emisión del fallo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Servicios de Seguridad – Continuidad Operativa
Partida 1.

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Documento con el diseño de alto nivel de las soluciones de seguridad a implementar en los centros de datos o donde lo indique el Instituto	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar	1% 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	1% 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 después de la finalización de la habilitación de todos los componentes en los Centros de Datos, o en el lugar designado por el Instituto, según lo establecido para cada solución integrada y una vez completada la	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

	integración de las mesas de trabajo.		
Memorias técnicas actualizadas de los servicios de seguridad	20 días hábiles antes de la finalización del contrato para aquellos servicios que estén habilitados.	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Servicios de Seguridad – Verificación/Calidad

Partida 1.

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Documento con el diseño de Alto Nivel de los servicios de Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integran activos de infraestructura para su habilitación	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar	1% 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	1% 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	1% 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	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Procedimientos de Operación del servicio • Servicios de Borrado Seguro de Información • Servicio de Gestión de Dominios • Servicio de Certificados Digitales SSL	10 días hábiles posteriores a la integración de las mesas de trabajo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
• Servicios de Ciberinteligencia (Ciberseguridad) • Servicios de Protección en Redes Inalámbricasy Seguridad en Dispositivos Móviles • Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA) • Servicios de Antivirus • Servicios de Prevención de Perdida de Información			
Metodología de implementación 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 posteriores a la integración de las mesas de trabajo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Partida 2.

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Procedimientos de Operación del servicio • Servicio de Análisis de Vulnerabilidades Estático • Servicio de Análisis de Vulnerabilidades Dinámico • Servicios de Análisis Forense • Servicio de Pruebas de Penetración	10 días hábiles posteriores a la integración de las mesas de trabajo	1% 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)
Partida 1.

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Procesos de operación implementados: Requerimientos Cambios Configuraciones Incidentes Problemas Monitoreo	15 días naturales posteriores a la emisión del fallo	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Matriz de Escalación Técnica y Organizacional	15 días naturales posteriores a la emisión del fallo	1% por cada día hábil 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 emisión del fallo	1% por cada día hábil 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	1% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

- **Deducciones**

Operbes S.A. de C.V. tomó en consideración que en términos de los artículos 53 Bis de Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 97 de su Reglamento, en caso de incumplimiento parcial o deficiente en la prestación del servicio por causas imputables a Operbes S.A. de C.V., El IMSS aplicará deducciones sobre el monto mensual facturado por pago del servicio de acuerdo con lo siguiente:

Durante la vigencia del contrato, al presentarte una falla, incidente, atención de requerimientos, ventana de mantenimiento, entre otras, y la causa raíz de estos eventos es atribuible a un tercero, no se aplicará una deducción a Operbes S.A. de C.V. en caso ser el proveedor de SASI 2025 por el servicio relacionado, siempre y cuando pueda demostrar con pruebas concretas que el servicio en cuestión se brindó conforme a las especificaciones del anexo técnico y los términos y condiciones acordados.

Operbes S.A. de C.V. tomó en consideración que el monto máximo de las deductivas, por ningún motivo podrán exceder del monto de la garantía de cumplimiento del contrato.

Conforme a lo anterior, en los casos en que las fallas, incidentes, atención de requerimientos, ventanas de mantenimiento, u otras eventualidades, sean atribuibles a la prestación de los servicios de seguridad por parte de Operbes S.A. de C.V., se aplicarán deducciones según los siguientes rubros:

Disponibilidad

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

Partida 1.

La disponibilidad se define como el porcentaje de tiempo durante el cual el sistema que proporciona el servicio de seguridad de SASI 2025, o cualquier componente de este, cumple con su función designada. En otras palabras, la disponibilidad representa la proporción de tiempo en la que el sistema opera según su propósito previsto, en comparación con el tiempo en el que debería haber estado operativo.

Las mediciones de disponibilidad serán realizadas porOperbes S.A. de C.V. en caso de ser el Proveedor de SASI 2025, utilizando las herramientas correspondientes de monitoreo del servicio y gestión de incidentes, con el objetivo de obtener mediciones precisas de los periodos operativos y no operativos, así como de sus causas.

Estas mediciones de disponibilidad se llevarán a cabo desde el inicio del período operativo de los servicios de seguridad "SASI 2025", para todos los módulos o posiciones de servicio contratados.
Operbes S.A. de C.V. se compromete a garantizar la disponibilidad con base en los siguientes factores:

- Se incluyen todos los componentes WAN, LAN, dispositivos de seguridad y otros dispositivos que respaldan el servicio de seguridad, así como su configuración lógica equivalente.

El método de medición se basará en una correlación de los datos recopilados cada 5 minutos por el sistema de monitoreo, con los períodos de indisponibilidad identificados en los incidentes abiertos en el sistema de gestión de incidencias de Operbes S.A. de C.V. en caso de ser el proveedor de SASI 2025. Se excluirán los períodos de indisponibilidad cuya responsabilidad no sea atribuible a Operbes S.A. de C.V. en caso de ser el Proveedor de SASI 2025. El procedimiento de medición se describe de la siguiente manera:

- Se calcula con base en un período mensual de 30 días.
- Se calcula a partir del inicio de la falla.
- Se considera que está indisponible cuando el protocolo de la interfaz está inactivo (Down) o cuando hay una caída de tráfico atribuible a la infraestructura de Operbes S.A. de C.V.
- Solo se calcula con base en base fallas atribuibles a Operbes S.A. de C.V.

Disponibilidad por sitio y por posición de servicio

Las interrupciones causadas por fallos de energía que sean responsabilidad del Instituto no se considerarán en el cálculo de la disponibilidad.

$$\text{Disponibilidad_del_Servicio} = \left[\frac{\text{Tiempo_Total} - (\text{Tiempo_Indisponible} - \text{Tiempo_Instituto})}{\text{Tiempo_Total}} \right] X100$$

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

Objetivos de la métrica:

Disponibilidad Servicio	% Disponibilidad

ANEXOS
DIVISIÓN DE CONTRATOS

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

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%

Deducción por incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Cuando no se cumplan con los objetivos de servicio, para los diferentes niveles de disponibilidad, conforme al esquema de medición propuesto	% de 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

Tiempo de detección y solución de fallas

Partida 1.

La métrica de tiempo de solución a fallas es independiente de la métrica de disponibilidad, ya que se refiere al lapso en el cual uno o varios servicios serán restituidos a su funcionamiento normal luego de presentarse una falla. Las mediciones del Tiempo de Solución de Fallas serán llevadas a cabo por Operbes S.A. de C.V., utilizando su herramienta correspondiente de gestión y monitoreo del servicio. Operbes S.A. de C.V. efectuará dichas mediciones de manera mensual, tomando en cuenta el promedio del tiempo requerido para resolver cada tipo de severidad. La metodología por emplear, así como las herramientas y los responsables de las mediciones, serán definidos en las mesas de trabajo.

El Tiempo de Solución a Fallas se clasifica en cuatro categorías, según la severidad, causa e impacto de estas:

Severidad Crítica: Denota un incidente de alto impacto debido al riesgo que implica. Este tipo de incidente tiene el potencial de causar afectaciones y daños significativos en los activos y servicios del cliente. Puede incluir eventos como la interrupción total del servicio, la pérdida completa del sistema de comunicaciones y/o seguridad, la degradación de los recursos del Instituto, o la identificación de vulnerabilidades en la infraestructura protegida. Se considera una alarma significativa en el sistema de gestión cuando persiste durante más de 10 minutos.

Severidad Alta: Describe un incidente significativo en el que se experimenta una degradación, aunque no necesariamente una interrupción en los servicios e infraestructura protegidos por dispositivos de alta disponibilidad o seguridad. Este tipo de incidente se manifiesta a través de bloqueos o un rendimiento deficiente al intentar acceder a ciertos servicios de red que dependen de los dispositivos de comunicación y/o seguridad. También puede implicar la pérdida parcial de funcionalidades en el equipo de comunicaciones y/o seguridad. Estos eventos causan una degradación en el servicio sin llegar a provocar su interrupción completa.

Severidad Media: Este tipo de incidente se considera menor ya que no tiene un impacto significativo en los servicios o infraestructura protegidos por los dispositivos de seguridad. Por lo general, involucra problemas como fallas en la visualización de registros de actividad o dificultades en la comunicación entre servicios

internos del Instituto y un grupo reducido de usuarios. Estos eventos suelen resultar en interrupciones en la disponibilidad del servicio durante períodos de tiempo cortos, generalmente inferiores a 10 minutos.

Severidad Baja: Estos casos se clasifican como preventivos con el propósito de mejorar u optimizar cualquier servicio de seguridad. La atención de estos casos de baja severidad será llevada a cabo por ingenieros de Operbes S.A. de C.V. en el sitio, con la colaboración del fabricante a través de un centro de asistencia técnica personalizada. El tiempo de resolución de este tipo de incidencias será acordado entre el Instituto y Operbes S.A. de C.V. al momento de presentarse el caso.

Operbes S.A. de C.V. tomó en consideración que la severidad de un incidente es determinada por el Instituto . Se establece la severidad, así como su nivel de escalación, en función de la operación y la criticidad de un servicio, basándose en los siguientes criterios:

SEVERIDAD	AFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
Critica	Una falla de alto impacto representa un problema crítico que impide por completo la operación de un servicio vital, el cual es fundamental para respaldar una función empresarial del Instituto a nivel nacional.	10 minutos posteriores a la detección de la falla	2 horas posteriores al registro y notificación de la falla
Alta	Se trata de un fallo que ocasiona una degradación en el servicio, impidiendo su correcto funcionamiento. Este servicio es crucial para respaldar una función de negocio dentro del Instituto, aunque su impacto se limita a nivel local y no afecta a escala nacional.	20 minutos posterior a la detección de la falla	4 horas posterior al registro y notificación de la falla
Media	Se trata de una falla menor que afecta la operación de un servicio específico del Instituto, impactando a un reducido grupo de usuarios.	120 minutos posterior a la detección de la falla	48 horas posterior al registro y notificación de la falla
Baja	Se consideran casos preventivos que buscan mejorar u optimizar cualquier servicio de seguridad. Estos casos tienen un impacto mínimo en la operación del negocio y pueden ser atendidos o resueltos según un calendario establecido.	5 días hábiles posterior a la detección de la falla	Se establecerá un acuerdo entre el Instituto y Operbes S.A. de C.V. en caso de ser el Proveedor de SASI 2025, conforme a las mesas de trabajo que se establezcan con este fin.

Deducción por incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de registro y notificación conforme al nivel de severidad critica	10 minutos posteriores al registro y notificación de la falla	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de solución conforme al nivel de severidad critica	2 horas posteriores al registro y notificación de la falla	Hora	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad alta	20 minutos posteriores al registro y notificación de la falla	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad alta	4 horas posteriores a la registro y notificación de la falla	Hora	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad media	120 minutos posteriores al registro y notificación de la falla	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad media	48 horas posteriores al registro y notificación de la falla	Hora	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad baja	5 días hábiles posteriores al registro y notificación de la falla	Día	0.2% por cada día hábil de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad baja	Se define entre el Instituto y Operbes S.A. de C.V. en caso de ser el Proveedor de SASI 2025 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
Partida 1.

Un incidente es aquel evento, que, de materializarse, podrían comprometer la seguridad de la red y los activos de información que componen las misma, así como las aplicaciones que dan tratamientos a información de usuarios externos e internos.

De igual manera una actividad sospechosa es aquel evento que, de materializarse, podría comprometer la seguridad de la información, convirtiéndose en un incidente de seguridad.

Los incidentes se definen como la constatación de una violación a las políticas de seguridad informática o al uso aceptable de prácticas y políticas de seguridad estandarizadas, representando una evidencia clara de la vulneración de la confidencialidad, integridad y disponibilidad de la información, misma que puede presentarse por un factor externo, como por la ejecución incorrecta a través de un recurso interno (SOC).

Las métricas de tiempo relacionadas con el registro y la notificación se refieren al periodo en el que Operbes S.A. de C.V. en caso de ser el proveedor SASI 2025 informa al Instituto sobre la confirmación de un incidente de seguridad. Estas métricas deben cumplirse según la prioridad establecida a partir de la apertura de un

registro vinculado a un incidente de seguridad. Respecto al tiempo de contención, se espera que Operbes S.A. de C.V. en caso de ser el Proveedor de SASI 2025 detenga y aísle el incidente tras su detección, de acuerdo con los tiempos definidos para cada nivel de prioridad.

Todas estas mediciones serán llevadas a cabo por Operbes S.A. de C.V. en caso de ser el proveedor de SASI 2025 utilizando las herramientas correspondientes de gestión y monitoreo del servicio. Además, Operbes S.A. de C.V. realizará estas mediciones de manera mensual, conforme al nivel de servicio establecido para cada tipo de métrica y/o prioridad.

Objetivos de la métrica

SEVERIDAD	AFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
Critica	Se refiere a un incidente de gran impacto que interrumpe por completo la operación de un servicio vital para una función empresarial del Instituto a nivel nacional.	10 minutos posteriores a la detección del incidente	60 minutos posteriores al registro y notificación del incidente
Alta	Se refiere a un incidente que ha provocado una degradación en el servicio, impidiendo su correcta operación. Este servicio es crucial para respaldar una función de negocio dentro del Instituto, aunque es importante destacar que su impacto se limita a nivel local y no afecta a nivel nacional.	20 minutos posterior a la detección del incidente	240 minutos posteriores al registro y notificación del incidente
Media	Se trata de un incidente menor que afecta a un pequeño grupo de usuarios del Instituto, impidiendo temporalmente el normal funcionamiento de un servicio.	30 minutos posterior a la detección del incidente	60 minutos posteriores al registro y notificación del incidente
Baja	Estos casos se consideran preventivos con el objetivo de mejorar u optimizar cualquier servicio de seguridad. Tienen un impacto mínimo en la operación del negocio y su atención y/o solución puede ser programada con antelación.	60 minutos posterior a la detección del incidente	2,880 minutos posteriores al registro y notificación del incidente

Deducción por incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de registro y notificación conforme al nivel de severidad critica	10 minutos posteriores al registro y notificación del incidente	Minuto	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad critica	60 minutos posteriores al registro y notificación del incidente	Minuto	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad alta	20 minutos posteriores al registro y notificación del incidente	Minuto	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad alta	240 minutos posteriores al registro y notificación del incidente	Minuto	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación	30 minutos posteriores al registro y notificación del incidente	Minuto	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
conforme al nivel de severidad media				
Tiempo máximo de solución conforme al nivel de severidad media	1,440 minutos posteriores al registro y notificación del incidente	Minuto	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad baja	60 minutos posteriores al registro y notificación del incidente	Minuto	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad baja	2,880 minutos posteriores al registro y notificación del incidente	Minuto	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Solicitudes de requerimientos y cambios

Partida 1

Consiste en el tiempo requerido por Operbes S.A. de C.V. en caso de ser el Proveedor de SASI para llevar a cabo altas, cambios o bajas en la infraestructura del servicio de seguridad. Estas acciones se basarán en un conjunto de configuraciones preestablecidas, definidas durante las correspondientes mesas de trabajo. Dichas configuraciones serán diseñadas para satisfacer las necesidades de conectividad y flujos de información de las aplicaciones del Instituto. Se reconoce que la complejidad en la atención de estas tareas es mínima, dado que se cuenta con experiencia y conocimiento previo sobre las mismas configuraciones utilizadas en los módulos de los servicios de seguridad actualmente en funcionamiento.

Objetivos de la métrica

PRIORIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE EJECUCIÓN
Alta	Solicitud generada por el Instituto para abordar necesidades operativas urgentes.	10 minutos posteriores a la solicitud formal por parte del Instituto	60 minutos posteriores al registro realizado por el Instituto
Media	Solicitud emitida por el Instituto para atender necesidades operativas habituales.	30 minutos posteriores a la solicitud formal por parte del Instituto	480 minutos posteriores al registro realizado por el Instituto
Baja	Solicitud generada por el Instituto para abordar necesidades operativas planificadas.	60 minutos posteriores a la solicitud formal por parte del Instituto	1,440 minutos posteriores al registro realizado por el Instituto

Cambios

Cualquier modificación realizada por Operbes S.A. de C.V., sin la autorización del Instituto, que resulte en una falla en los servicios de seguridad, será considerada como un incidente de seguridad. Este incidente será clasificado según las afectaciones o riesgos que haya generado.

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

PRIORIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE EJECUCIÓN
Emergente	Se requerirán cambios inmediatos en la infraestructura de la red en caso de experimentar una pérdida repentina del servicio, fallo en cualquiera de los activos de infraestructura, o a solicitud expresa del Instituto.	1 hora posteriores a la solicitud formal por parte del Instituto	Conforme al plan de trabajo definido entre el Instituto y Operbes S.A. de C.V.
Normal	Modificaciones necesarias para mejorar o restablecer un servicio o expandir un activo de infraestructura, que no están contempladas en el catálogo de cambios estándar, requieren un análisis y aprobación por parte del Instituto.	1 hora posteriores a la solicitud formal por parte del Instituto	Conforme al plan de trabajo definido entre el Instituto y Operbes S.A. de C.V.
Estándar	Actualizaciones en los servicios y/o activos de infraestructura que se ejecutan de manera online y siguen un proceso establecido, constituyendo una solución aceptada para un conjunto específico de requerimientos.	1 hora posteriores a la solicitud formal por parte del Instituto	24 horas posterior al registro realizado por el Instituto

Deducción por incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de registro y notificación conforme al nivel de prioridad Alta	10 minutos posteriores al registro y notificación del requerimiento	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de ejecución conforme al nivel de prioridad Alta	60 minutos posteriores al registro y notificación del requerimiento	Minuto	0.5% por cada minuto de atraso en la ejecución del requerimiento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Media	30 minutos posteriores al registro y notificación del requerimiento	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Media	8 horas posteriores al registro y notificación del requerimiento	Hora	0.5% por cada hora o fracción de atraso en la ejecución del requerimiento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Baja	60 minutos posteriores al registro y notificación del requerimiento	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Baja	24 horas posteriores al registro y notificación del requerimiento	Hora	0.5% por cada hora o fracción de atraso en la ejecución del requerimiento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

Cambios

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de registro y notificación conforme al nivel de prioridad Emergente	60 minutos posteriores al registro y notificación del cambio	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de ejecución conforme al nivel de prioridad Emergente	Conforme al plan de trabajo definido entre el Instituto y Operbes S.A. de C.V.	Hora	1% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Normal	60 minutos posteriores al registro y notificación del cambio	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Normal	Conforme al plan de trabajo definido entre el Instituto y Operbes S.A. de C.V.	Hora	1% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Estándar	60 minutos posteriores al registro y notificación del cambio	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Estándar	24 horas posteriores al registro y notificación del cambio	Hora	1% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Servicios de Seguridad – Continuidad Operativa

Partida 1.

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Reportes Técnicos de los activos de infraestructura que contemplen: ▪ 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 posteriores al cumplimiento del mes vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

Servicios de Seguridad – Verificación/Calidad

Partida 1.

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Reportes Técnicos de los activos de infraestructura que contemplen: ▪ Disponibilidad ▪ Controles de Cambios ▪ Requerimientos ▪ Incidentes/Falla ▪ Actividad Sospechosa ▪ Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	5 días hábiles siguientes al vencimiento del mes.	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 Borrado Seguro de Información: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado.	5 días hábiles siguientes al vencimiento del mes.	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicio de Gestión de Dominios: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos.	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicio de 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	1 día hábil posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
(incluyendo archivo electrónico compreso con la llave publica relacionado con los requerimientos)				
Servicios de Ciberinteligencia: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de amenazas y ataques potenciales a los que se encuentra expuesto el Instituto que incluya: Situación general del evento, hallazgos detectados, mecanismos de inteligencia accionable, táctica u operativa recomendados para prevención y/o contención	1 día hábil posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos Móviles: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las politicas, configuraciones o reportes solicitados por el Instituto	1 día hábil posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA): Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las politicas, configuraciones o reportes solicitados por el Instituto	5 días hábiles posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Antivirus: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las politicas, configuraciones o reportes solicitados por el Instituto.	1 día hábil posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Prevención de Pérdida de Información: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las politicas, configuraciones o	1 día hábil posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
reportes solicitados por el 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	10 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del plan de trabajo	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Sistema de Gestión de Seguridad de la Información: Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora del Sistemas De Gestión de Seguridad de la Información (SGSI)	Conforme a la fecha estipulada en el plan de trabajo acordado entre el Instituto y Operbes S.A. de C.V.	Día	1% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, por evento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Gestión del Cambio en Seguridad de la Información: Plan de Trabajo de implementación y operación de los servicios conforme al alcance definido en las mesas de trabajo	10 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del plan de trabajo	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Gestión del Cambio en Seguridad de la Información: Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora de la Gestión del Cambio en Seguridad de la Información	Conforme a la fecha estipulada en el plan de trabajo acordado entre el Instituto y Operbes S.A. de C.V.	Día	1% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, por evento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Servicios del Centro de Operaciones de Seguridad (SOC)

Operbes S.A. de C.V. tomó en consideración que cualquier modificación realizada por el SOC, sin autorización previa del Instituto, ya sea que cause o no una falla en los servicios de seguridad, se considerará como un incidente de seguridad. Este incidente será clasificado según las afectaciones o riesgos que pueda haber ocasionado.

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	5 días hábiles siguientes al término 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 siguientes al término 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 siguientes al término 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 siguientes al término 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 siguientes al término del mes vencido.	Día	1% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte de las evaluaciones operativas a los servicios de seguridad implementados	5 días hábiles posteriores al cumplimiento del trimestre vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte que integre el calendario de actualizaciones de versionamiento en software de cada servicio implementados	5 días hábiles posteriores al cumplimiento del trimestre vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Creación de cuentas de acceso en las consolas de administración de los servicios de seguridad	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto	Día	1% por cada día hábil de atraso en la entrega de las cuentas de acceso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a	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

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
	cada solicitud generada por el Instituto			
Actualización de la matriz de escalación	5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad	Día	1% por cada día hábil de atraso en la entrega de la matriz de escalación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad	5 días hábiles posteriores a la ejecución de la ventana mantenimiento	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de las configuraciones de las soluciones de seguridad	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de los incidentes presentados en las soluciones de seguridad	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de los requerimientos registrados en la mesa de servicios	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y su diagrama de interrelación conforme fueron registrados en la CMDB	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Diagramas de Arquitectura de las soluciones de seguridad	2 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tablero de Estadísticas de Servicios de Seguridad (Portal Único)	10 días hábiles posteriores al término de la habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo	Día	1% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, por evento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

11. Mecanismos requeridos al proveedor para responder por defectos o vicios ocultos de los bienes o de la calidad de los servicios.

Operbes S.A. de C.V. tomó en consideración que no aplica

12. Garantías de anticipos y cumplimiento.

Operbes S.A. de C.V., para garantizar el cumplimiento de todas y cada una de las obligaciones estipuladas en el contrato adjudicado, de conformidad con lo establecido en el numeral 4.30.1 de las POBALINES, presentará copia simple de la fianza expedida por afianzadora debidamente constituida en términos de la Ley de Instituciones de Seguros y de Fianzas, por un importe equivalente al 10% (diez por ciento) del monto máximo del contrato, sin incluir el impuesto al Valor Agregado, a favor del Instituto Mexicano del Seguro Social, la cual será divisible.

La vigencia de la fianza quedara abierta durante la vigencia del contrato para permitir que cumpla con su objetivo.

Operbes S.A. de C.V. en término de lo dispuesto en el artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, deberá entregar al INSTITUTO MEXICANO DEL SEGURO SOCIAL dentro de los 10 (diez) días naturales siguientes a la firma del contrato el original de la fianza a la División de Contratos, ubicada en Calle Durango número 291, 10º piso, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700 Ciudad de México.

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

a) Plazo para notificar al proveedor.

La garantía de cumplimiento del contrato se presentará en el plazo o fecha previstos en la convocatoria a la licitación; en su defecto, a más tardar dentro de los diez días naturales siguientes a la firma del contrato.

b) La existencia de consumibles y refacciones, en su caso.

Operbes S.A. de C.V. tomó en consideración que no aplica

c) Plazo y condiciones de canje o devolución del bien.

Operbes S.A. de C.V. tomó en consideración que no aplica

d) Caducidad de los bienes.

Operbes S.A. de C.V. tomó en consideración que no aplica

e) Centros de servicio (domicilios y horarios) y reporte técnico.

Operbes S.A. de C.V. tomó en consideración que no aplica

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

f) Periodo de garantía.

Operbes S.A. de C.V. tomó en consideración que durante la vigencia del contrato

g) Tiempos máximos de reparación o atención de fallas.

Operbes S.A. de C.V. tomó en consideración que conforme lo establecido en el documento de términos y condiciones, en su numeral 10.Penas convencionales y deductivas.

h) Garantía de mano de obra y/o partes.

Operbes S.A. de C.V. tomó en consideración que no aplica

i) Mantenimientos correctivos y/o preventivos.

Operbes S.A. de C.V. tomó en consideración que no aplica

j) En su caso, si se requiere capacitación, solicitar programa para la misma.

Operbes S.A. de C.V. tomó en consideración que no aplica

k) Porcentaje a requerir por concepto de garantía de cumplimiento.

Operbes S.A. de C.V. tomó en consideración que por un importe equivalente al 10% (diez por ciento) del monto máximo del contrato, sin considerar el impuesto al valor agregado, a favor del Instituto.

13. Forma de pago.

Operbes S.A. de C.V. tomó en consideración que el servicio descrito en el Anexo Técnico de las bases está modelado con base en un esquema de pago unitario mensual conforme a las entregas programadas, el cual se realizará en moneda nacional y conforme al siguiente esquema:

Operbes S.A. de C.V. tomó en consideración que reportará y solicitará al Instituto el pago asociado al servicio que éste ha entregado y que esté funcionando conforme a las especificaciones descritas en el Anexo Técnico de la bases, y con estricto apego a las características y niveles de servicio que se requieren para cada rubro definido, sujeto a posibles deducciones por incumplimiento de los mismos, por lo que el IMSS, a través del Administrador del Contrato, evaluará las condiciones de funcionalidad y operatividad de los servicios entregados por Operbes S.A. de C.V. para que proceda el pago mensual que debe efectuarse por los mismos.

14. Mecanismos de comprobación, supervisión y verificación de los bienes o de los servicios contratados.

Para este fin, se llevarán a cabo reuniones mensuales en las que se revisará la operación de Operbes S.A. de C.V. en caso de ser el licitante adjudicado, comparándola con los indicadores de niveles de servicio acordados. Esta evaluación se plasmará en un documento denominado 'Acta Administrativa de Entrega-Recepción Mensual de los Servicio Administrado de Seguridad de la Información SASI 2025. La periodicidad de esta acta será mensual desde el inicio de la prestación del servicio y se realizará dentro de los 5 días hábiles posteriores al cierre de cada mes.

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

En consecuencia, Operbes S.A. de C.V. reconoce expresamente que el servicio no será considerado como aceptado o recibido por parte del Instituto hasta que se cumpla conforme a lo establecido en los párrafos anteriores.

Todas las actas mencionadas en este apartado contarán con la firma de conformidad del Administrador del Contrato del IMSS y serán elaboradas en cuatro tantos originales: uno para Operbes S.A. de C.V. en caso de ser el licitante adjudicado, otro para el Administrador del Contrato, un tercero para el expediente de la Coordinación de Telecomunicaciones y Seguridad de la Información, y el último para la División de Trámite de Erogaciones.

15. Anticipo.

Operbes S.A. de C.V. tomó en consideración que el instituto no otorgará anticipos.

16. Aviso de privacidad y medidas de seguridad para el manejo de la información para bienes o servicios de TIC.

Operbes S.A. de C.V. tomó en consideración que no aplica

17. Seguro de Responsabilidad Civil.

Operbes S.A. de C.V. tomó en consideración que no aplica

18. Dictámenes de protección civil emitidos por las autoridades competentes en la materia.

Operbes S.A. de C.V. tomó en consideración que no aplica

19. Confidencialidad

Tanto el Instituto como Operbes S.A. de C.V. acuerdan considerar como información confidencial todo material, impreso o electrónico, que contenga datos, grabaciones, programas de cómputo o cualquier otro contenido vinculado a información jurídica, operativa, técnica, financiera, análisis, registros, documentos, especificaciones, productos, informes, dictámenes o desarrollos, tanto aquellos a los que tenga acceso como los proporcionados durante la prestación del servicio. Asimismo, se considerará como confidencial toda la información facilitada por el Instituto Mexicano del Seguro Social para la ejecución del servicio y que sea exclusiva propiedad del Instituto Mexicano del Seguro Social.

Operbes S.A. de C.V. reconoce que está terminantemente prohibida la divulgación total o parcial de esta información a su favor o a terceros ajenos a la relación contractual, por cualquier medio disponible, incluyendo, de manera enunciativa mas no limitativa, vía oral, impresa, electrónica, magnética, óptica, o cualquier otro medio, conforme a los plazos establecidos en la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables en la materia."

Operbes S.A. de C.V. reconoce y acepta la prohibición mencionada en el párrafo anterior, comprendiendo que está absolutamente prohibido divulgar la información del Instituto con fines de lucro, comerciales, académicos, educativos u otros ajenos al propósito de la presente contratación. En consecuencia, Operbes S.A. de C.V. asume la responsabilidad del uso y cuidado de la información.

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

En virtud de lo anterior, Operbes S.A. de C.V. se compromete a mantener una estricta confidencialidad sobre la información a la que acceda, asegurando que cada miembro del personal asignado para el desarrollo y operación del proyecto respete el manejo adecuado de dicha información.

Operbes S.A. de C.V. tomó en consideración que considerar como confidencial toda la información a la que tenga acceso el personal designado para prestar los servicios objeto de esta contratación. Operbes S.A. de C.V. se compromete a garantizar que dicho personal no copie ni respalde información del Instituto Mexicano del Seguro Social en ningún equipo sin la previa autorización por escrito por parte del **Instituto**.

Operbes S.A. de C.V. tomó en consideración que Garantizar que el acceso a la información del Instituto Mexicano del Seguro Social esté restringido únicamente al personal autorizado por el Instituto. El incumplimiento de estas condiciones será considerado como una violación de la confidencialidad y protección de datos personales.

Además, Operbes S.A. de C.V. tomó en consideración que cualquier persona que tenga acceso a esta información será informada y comprometida a cumplir con lo establecido en el Anexo Técnico de esta contratación.

Es importante destacar que la información proporcionada por el Instituto a Operbes S.A. de C.V. para la prestación del servicio no otorgará a Operbes S.A. de C.V. titularidad o derechos de autor, ni de ninguna otra índole.

Operbes S.A. de C.V. será responsable en el caso de que se violen derechos de propiedad industrial, patentes o derechos de autor, respecto al software y/o hardware utilizados para brindar el servicio, dejando en todo momento a salvo a el Instituto.

20. Propiedad intelectual

Durante el período de garantía de las licencias, Operbes S.A. de C.V. se compromete a eximir al Instituto de cualquier responsabilidad de índole civil, mercantil, penal o administrativa que pudiera surgir como resultado de la violación de derechos de autor, patentes, marcas u otros derechos de propiedad industrial o intelectual, tanto a nivel nacional como internacional. Esta exención de responsabilidad abarca cualquier reclamo, demanda, acción legal o procedimiento que pueda surgir contra el Instituto como consecuencia de dicha infracción. Además, Operbes S.A. de C.V. se compromete a asumir todos los costos, gastos, multas o indemnizaciones que puedan derivarse de tales reclamaciones, eximiendo al Instituto de cualquier carga económica asociada a las mismas.

21. Tipo de abastecimiento.

Operbes S.A. de C.V. tomó en consideración que el tipo de abastecimiento será mediante dos partidas.

22. Modalidad del contrato

Operbes S.A. de C.V. tomó en consideración que el Contrato de modalidad abierta.

ANEXOS
DIVISIÓN DE CONTRATOS

Propuesta Técnica
Terminos y Condiciones

Servicios Administrados de Seguridad Informática (SASI) 2025

23. Área Requirente y Técnica

Operbes S.A. de C.V. tomó en consideración que el Área Requirente: El Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información.

Operbes S.A. de C.V. tomó en consideración que el Área Técnica: El Titular de la División de Seguridad Informática Física.

24. Administrador del contrato y responsable de la supervisión del mismo

Operbes S.A. de C.V. tomó en consideración que el Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información.

Propuesta Técnica

Operbes, S.A. de C.V. participa en la Partida 1

ANEXOS
DIVISIÓN DE CONTRATOS

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

Contenido

I. Objetivo del Documento 3
II. Características y especificaciones. 3
i. Alcance 4
III. Requerimientos técnicos 5
IV. Especificaciones técnicas 5
Partida 1. 5
iv.1 Servicios de Seguridad – Continuidad Operativa 5
iv.1.2 Servicios de Prevención de Intrusos (IPS) 6
iv.1.3 Servicios de Protección contra Denegación de Servicio (DDoS) 7
iv.1.4 Servicios de Redes Privadas Virtuales (VPN) 9
iv.1.5 Servicios de Filtrado de Contenido Web 10
iv.1.6 Servicios de Filtrado de Contenido de Correo (Antispam) 12
iv.1.7 Servicios de Firewall Especializado en Servicios Web (WAF) 13
iv.1.8 Servicios de Firewall especializado en Base de Datos (DBF) 14
iv.1.9 Servicios de Gestión Unificada de Amenazas (UTM) 15
iv.1.10 Servicio de Correlación de Eventos 16
iv.1.11 Servicio de Protección de Amenazas Persistentes Avanzadas (APT) 18
iv.2 Servicios de Seguridad – Verificación y Calidad 19
iv.2.1 Servicios de Borrado Seguro de Información 19
iv.2.2 Servicio de Gestión de Dominios 20
iv.2.3 Servicio de Certificados Digitales SSL 21
iv.2.4 Servicios de Ciberinteligencia (Ciberseguridad) 21
iv.2.5 Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos Móviles. 23
iv.2.6 Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA). 23
iv.2.7 Servicio de Antivirus 25
iv.2.8 Servicios de Prevención de Pérdida de Información 26
iv.2.9 Servicios de Sistema de Gestión de Seguridad de la Información (SGSI) 27
iv.2.10 Servicios Continuidad de Gestión del Cambio en Seguridad de la Información 30
iv.2.10 Servicios del Centro de Operaciones de Seguridad (SOC) 31
V. Perfil de Operbes S.A. de C.V. 37
VI. Condiciones técnicas de aceptación de entregable 38
VII. Cronograma de actividades 45
VIII. Niveles de servicio acordados que se cumplirán 45
IX. Requerimientos de arquitectura tecnológica 47
X. Restricciones e interfaces con otros elementos 47
XI. Pruebas requeridas, método de evaluación y el resultado mínimo que se obtendrá al ejecutar las pruebas. 47
XII. Modificaciones de la especificación técnica de algún bien que no se encuentre regulado por el compendio nacional de insumos para la salud. 47
XIII. Modificaciones de la especificación técnica de un bien respecto de las estipuladas en el ejercicio anterior. 47
XIV. Normas: Oficial Mexicana, Estándar (antes mexicana), Internacional, de Referencia o Especificación Técnica, que resulte aplicable a los bienes o servicios requeridos. 47

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

I. Objetivo del Documento

Operbes S.A. de C.V. oferta el servicio tomando en consideración todo lo establecido en las especificaciones técnicas, calendarios y lineamientos para la contratación de los Servicios Administrados de Seguridad Informática para el ejercicio 2025, en lo sucesivo EL SERVICIO.

a) Descripción amplia y detallada de los bienes a adquirir o arrendar o servicios solicitados.

Operbes S.A. de C.V. , oferta el servicio con la clave del Clasificador Único de las Contrataciones Públicas (CUCOP) de los bienes a adquirir o arrendar o servicios solicitados se identifica en la siguiente tabla:

Clave CUCOP	31900004
Descripción	Servicios a centros de datos (hospedaje, electricidad, video vigilancia, monitoreo, aire acondicionado, servidores y otros
Unidad de Medida	Servicio
Partida Específica (COG)	31904 "Servicios Integrales de Infraestructura de Computo"
Objetivo del contrato	Servicios Administrados de Seguridad Informática

II. Características y especificaciones.

Operbes S.A. de C.V. tomó en consideración que el SERVICIO se encuentra dividido en 2 (dos) partidas, las cuales operarán de manera integrada y unificada y se adjudicarán por partida a un único licitante, cuya propuesta cumpla con todos los requisitos obligatorios y obtenga la mayor puntuación en la evaluación combinada de puntos o porcentajes.

Operbes S.A. de C.V., oferta la partida 1 (uno) Servicios de Seguridad – Continuidad Operativa

Debido a la naturaleza técnica del SERVICIO, Operbes S.A. de C.V., acepta que los licitantes solo podrán participar en una de las dos partidas. Esta restricción se establece para evitar conflictos de interés técnico que pudieran afectar al IMSS.

Operbes S.A. de C.V., acepta que las partidas incluyen:

1. **Toma en Operación y Transición:** Esto incluirá la implementación de procesos de cambio, gestión de riesgos y capacitación del personal para asegurar una transición eficiente.
2. **Servicios de Infraestructura:** Incluye la operación, soporte y mantenimiento de la infraestructura existente, así como la implementación y gestión de infraestructura para los centros de datos. Además, proporcionará atención a los servicios y aplicaciones del instituto. Se asegurará que la infraestructura sea confiable, segura y capaz de satisfacer las necesidades operativas del IMSS.
3. **Protección Integral de Servidores, Aplicaciones y Bases de Datos:** Se brindará un servicio completo de protección para los servidores, aplicaciones y bases de datos del IMSS. Esto incluirá medidas preventivas y reactivas para garantizar la integridad y disponibilidad de los datos críticos. Se implementarán soluciones avanzadas de seguridad para hacer frente a las amenazas actuales y emergentes.
4. **Servicios de Seguridad de la Información Especializados:** Este servicio se centrará en aspectos específicos relacionados con las tecnologías de la información, comunicaciones y seguridad de la información.

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

Objetivos específicos
Operbes S.A. de C.V., oferta los siguientes objetivos:

- Salvaguardar y proteger la información institucional.
- Garantizar la continuidad operativa, de negocio y la seguridad de la información durante la vigencia del presente contrato, especialmente durante la transición del contrato anterior a los servicios de SERVICIO.
- Reforzar la seguridad de la información contra posibles amenazas, reduciendo el riesgo de incidentes de seguridad mediante la aplicación de tecnología de vanguardia para la supervisión, detección, aseguramiento, contención y respuesta ante posibles ataques a la infraestructura de cómputo, sistemas y aplicaciones del IMSS.
- Contar con servicios de infraestructura regulados por niveles de servicio que incluyan la implementación de componentes necesarios en los centros de datos y servicios del IMSS, así como la gestión integral de la infraestructura para satisfacer las necesidades de conectividad, comunicación, protección, control y filtrado de la institución, asegurando que la plataforma tecnológica opere en óptimas condiciones.
- Disponer de servicios de protección de manera unificada e integrada, incluyendo la prevención de pérdida de información, protección de sistemas físicos o virtuales, protección del correo electrónico interno y externo, herramientas de colaboración y trazabilidad, así como el filtrado e inspección del acceso a internet e intranet mediante una solución integral que permita la gestión consolidada de funcionalidades y servicios, con el fin de mantener, asegurar y fortalecer el esquema de seguridad del IMSS.
- Contar con servicios de seguridad de la información que complementen de manera consistente y robusta el esquema de seguridad institucional, incluyendo el control, aseguramiento, diagnóstico, pruebas, metodologías, acceso a cuentas privilegiadas, bases de datos, aplicaciones, correlación y trazabilidad de eventos, investigación forense y otros servicios especializados en seguridad y tecnologías de la información.

i. Alcance

Operbes S.A. de C.V., oferta el alcance del SERVICIO el cual incluye los siguientes aspectos:

1. Un esquema de servicios para la implementación, gestión y monitoreo de la infraestructura física y de seguridad necesaria para la integración de los centros de datos. Este esquema se caracteriza por una arquitectura flexible que se adapta a las necesidades de migración. Incluye la operación, soporte y mantenimiento de la infraestructura existente, así como la posibilidad de su sustitución para mantener una plataforma tecnológicamente moderna y uniforme, garantizando la continuidad operativa, empresarial y la seguridad de la información del IMSS.
2. Un esquema de servicios de protección que ofrece una solución integral, cubriendo la protección de los servicios de colaboración internos, el correo electrónico externo y la navegación web. Este esquema detecta y protege contra amenazas avanzadas, previene la fuga de información y se gestiona de manera consolidada.
3. Un esquema de servicios de seguridad que complementa el esquema de protección. Incluye servicios orientados a firewalls, sistemas de prevención de intrusiones (IPS), filtrado de contenido, protección contra ataques de denegación de servicio distribuido (DDoS), antispam, firewall de aplicaciones web (WAF), protección de bases de datos (DBF), redes privadas virtuales (VPN) y la implementación y administración de nuevos servicios requeridos por el instituto. Además, se ofrece análisis de vulnerabilidades, análisis forense, pruebas de penetración, borrado seguro de información, aseguramiento de aplicaciones, ciberinteligencia, servicios de protección para redes inalámbricas y dispositivos móviles, gestión y control de acceso para usuarios privilegiados, correlación de eventos, protección contra amenazas persistentes avanzadas (APT), gestión de procesos de seguridad y servicios especializados en seguridad de la información. Este esquema proporciona una cobertura completa de seguridad.

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

III. Requerimientos técnicos

Operbes S.A. de C.V., oferta y acepta los requerimientos técnicos se encuentran integrados en el Anexo Técnico junto con sus Apéndices A y B de las bases del proceso.

1) Funcionales

Operbes S.A. de C.V. oferta y acepta que los requerimientos técnicos se encuentran integrados en el Anexo Técnico junto con sus Apéndices A y B de las bases de la proceso.

2) No funcionales

Operbes S.A. de C.V. oferta y acepta que los requerimientos no funcionales se encuentran integrados en los Términos y Condiciones de la bases del proceso.

IV. Especificaciones técnicas

Partida 1.

iv.1 Servicios de Seguridad – Continuidad Operativa

iv.1.1 Servicios de Firewall

Descripción del servicio: Operbes S.A. de C.V., oferta y acepta garantizar la continuidad operativa del servicio que proporciona seguridad y protección, incluyendo el control de acceso, filtrado y bloqueo contra ataques dirigidos a las aplicaciones, así como la inspección de paquetes a nivel de aplicación para identificar patrones de tráfico anómalo.

Por consiguiente, Operbes S.A. de C.V., oferta el cumplimiento con las siguientes especificaciones funcionales mínimas:

- Garantizar la continuidad operativa de los activos de infraestructura actualmente en uso por el Instituto, así como de aquellos que sea necesario implementar, mediante el suministro de soporte técnico, licenciamiento y otros recursos necesarios. Esto asegurará cumplir con los niveles de servicio establecidos en el apéndice B.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda para mantener la continuidad operativa del Instituto, conforme a lo especificado en el Apéndice A.
- Desarrollar en colaboración con el Instituto la estrategia de habilitación para mantener la continuidad operativa de los activos de infraestructura actuales o los que sean necesarios según las necesidades operativas del Instituto.
- Realizar las acciones requeridas para la instalación del equipo en los Centros de Datos correspondientes o en cualquier otra ubicación designada por el Instituto.
- Coordinar con el personal del Instituto, a través del administrador del contrato o del modelo de gobierno designado, las ventanas de mantenimiento necesarias para garantizar el correcto funcionamiento del servicio. No se podrán realizar cambios en los componentes de hardware o software sin la autorización correspondiente.
- Continuar con la integración de cada activo de infraestructura en su consola de administración centralizada, ya sea en modo stand alone o para la administración de todos los dispositivos, y asegurar que los registros de actividad de cada activo estén integrados en la solución de correlación de eventos del proyecto o en otra designada por el Instituto para este propósito.
- Garantizar que los activos de infraestructura cuenten con actualizaciones tecnológicas estables y validadas del sistema operativo, aplicaciones (firmware) y otros componentes necesarios.
- Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.

ANEXOS
DIVISIÓN DE CONTRATOS

- •Mantener el acceso a los servicios alojados en la capa de servidores de los centros de datos (DMZ), gestionando según el esquema de seguridad establecido y respetando la segmentación entre las diferentes zonas de seguridad.
- •Prevenir la explotación de vulnerabilidades y el ingreso de tráfico malicioso a las redes del Instituto.
- •Atender todos los requerimientos de cambio, incidencias/fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos para tal fin.
- •Monitorear todos los eventos registrados en la solución y emitir alertas sobre incidentes generados por los activos de infraestructura del servicio.
- •Notificar actividades sospechosas relacionadas con la violación de políticas y aquellas identificadas a través de funcionalidades habilitadas en la solución.
- •Informar sobre fallas relacionadas con el hardware de los activos de infraestructura provistos a través del servicio.
- •Gestionar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como realizar todas las renovaciones requeridas durante la vigencia de los servicios.
- •Realizar evaluaciones operativas de los servicios (herramientas de software y activos de infraestructura) y análisis de vulnerabilidades cada seis meses desde el inicio de operaciones y hasta seis meses antes del término de los servicios. Estas evaluaciones identificarán mejoras en el rendimiento de los activos, gestión de configuraciones y nuevas funcionalidades operativas derivadas de actualizaciones de hardware y/o software.
- •Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos, como componentes de comunicación entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- •Proporcionar al Instituto cuentas de acceso a las consolas de administración correspondientes al servicio, así como herramientas en software para acceder a las mismas, garantizando que sean de solo lectura y que los atributos de consulta se definan según las mesas correspondientes.
- •Suministrar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre casos de soporte, documentación técnica, pólizas de mantenimiento, licenciamiento adquirido y otros datos relevantes para la toma de decisiones sobre el uso del servicio.
- •Implementar un servicio de auditoría de reglas de acceso en los dispositivos firewall para el análisis y depuración de estas, mejorando así el control de acceso y la seguridad. Esta solución se ubicará en las instalaciones del centro de datos primario y no generará costos adicionales para el Instituto.
- Garantizar el cumplimiento de las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.2 Servicios de Prevención de Intrusos (IPS)

Descripción del servicio: Operbes S.A. de C.V., oferta y garantiza la continuidad operativa del servicio que proporciona protección perimetral basada en firmas y que identifica vulnerabilidades. Este servicio tiene como objetivo contener intentos de acceso no autorizado a los recursos o servicios publicados en Internet o Intranet que podrían afectar la operación de la organización, detectar accesos no autorizados y prevenir fugas de información.

Por lo tanto, Operbes S.A. de C.V. oferta el cumplimiento de las siguientes especificaciones funcionales mínimas:

• Garantizar la continuidad operativa de los activos de infraestructura actuales del Instituto o los que sean necesarios implementar, proporcionando el soporte técnico, licenciamiento u otros recursos necesarios para asegurar esta continuidad operativa, así como cumplir con los niveles de servicio requeridos, según lo establecido en el Apéndice B.

• Coordinar con el personal del Instituto, a través del administrador del contrato o del modelo de gobierno designado, las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio. No se podrán realizar cambios en los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por el Instituto.

• Continuar integrando cada activo de infraestructura en su consola de administración centralizada, ya sea en modo stand-alone para la administración de todos los dispositivos, y asegurar que los registros de actividad de cada activo estén integrados en la solución de correlación de eventos del proyecto o en otra designada por el Instituto.
• Garantizar que los activos de infraestructura cuenten con actualizaciones tecnológicas estables y validadas del sistema operativo, aplicaciones (firmware) y otros componentes necesarios.
• Permitir únicamente el tráfico definido por el Instituto, tanto interno como externo, entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.
• Prevenir la explotación de vulnerabilidades y el ingreso de tráfico malicioso a las redes del Instituto.
• Atender todos los requerimientos de cambio, incidentes/fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos.
• Monitorear todos los eventos registrados en la solución y emitir alertas sobre incidentes generados por los activos de infraestructura que componen el servicio.
•Notificar cualquier actividad sospechosa relacionada con la violación de políticas, así como aquellas identificadas mediante las funcionalidades habilitadas en la solución.
• Informar sobre fallas relacionadas con el hardware de los activos de infraestructura proporcionados a través del servicio.
• Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como llevar a cabo todas las renovaciones necesarias durante la vigencia de los servicios.
• Realizar evaluaciones operativas de los servicios y análisis de vulnerabilidades cada seis meses, desde el inicio de operaciones y hasta seis meses antes del término de estos, para identificar mejoras en el rendimiento de los activos, en la gestión de configuraciones y en la detección de nuevas funcionalidades operativas derivadas de actualizaciones de hardware y/o software.
• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en el presente propuesta Técnica, incluyendo componentes que faciliten la comunicación entre redes, el cableado eléctrico y de datos, el montaje en racks, entre otros.
• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas en software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otros disponibles), las cuales serán de solo lectura y cuyos atributos de consulta se definirán en las mesas establecidas para este propósito.
• Suministrar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licenciamiento adquirido para cada servicio proporcionado y otros datos relevantes para la toma de decisiones sobre el uso del presente servicio.
• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos IPS para el análisis y depuración de estas, así como para mejorar el control de acceso y la seguridad. Esta solución se implementará en las instalaciones del centro de datos primario y no generará costos adicionales para el instituto.
• Cumplir, como mínimo, con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.3 Servicios de Protección contra Denegación de Servicio (DDoS)
Descripción del servicio: Operbes S.A. de C.V. oferta mantener la continuidad operativa del servicio que brinda protección contra los ataques de denegación de servicio distribuido, basado en firmas y altos volúmenes de conexión.

Por lo tanto, Operbes S.A. de C.V., oferta el cumplimiento de las siguientes especificaciones funcionales mínimas:

ANEXOS
DIVISIÓN DE CONTRATOS

• Asegurar la continuidad operativa de los activos de infraestructura actuales del Instituto, proporcionando el soporte técnico, licenciamiento u otros recursos necesarios para garantizar esta continuidad operativa, así como cumplir con los niveles de servicio requeridos para este propósito, según lo establecido en el Apéndice B.
• Integrar una solución híbrida con activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, junto con una solución de nube para mantener la continuidad operativa del Instituto, conforme a lo dispuesto en el Apéndice A.
• Definir en colaboración con el Instituto la estrategia para habilitar la continuidad operativa de los activos de infraestructura actuales o los necesarios para cubrir las necesidades operativas.
• Realizar las tareas necesarias para instalar el equipo en los Centros de Datos correspondientes, o en cualquier otra ubicación solicitada por el Instituto.
• Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado, las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio. En ningún momento se podrán realizar cambios en los componentes de hardware o software que integran el servicio sin un control de cambios autorizado por el Instituto.
• Continuar integrando cada activo de infraestructura en su respectiva consola de administración centralizada, pudiendo ser en modo stand-alone para la administración de todos los dispositivos, y asegurar que la bitácora de cada activo esté integrada en la solución de correlación de eventos del proyecto o en otra designada por el Instituto.
• Garantizar que los activos de infraestructura cuenten con actualizaciones tecnológicas estables y validadas del sistema operativo, aplicación (firmware) y otros componentes necesarios.
• Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.
• Continuar con el acceso a los servicios ubicados en la capa de servidores de los centros de datos (DMZ), gestionando 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, incidentes/fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos para dicho propósito.
• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura que componen el servicio, incluyendo:
  - Notificar actividades sospechosas relacionadas con la violación de las políticas, así como las identificadas a través de las funcionalidades habilitadas en la solución.
  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura proporcionados a través del servicio.
• Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como realizar todas las renovaciones necesarias durante la vigencia de los servicios.
• Realizar evaluaciones operativas a los servicios (herramienta de software y activos de infraestructura), así como análisis de vulnerabilidades, para identificar mejoras en el desempeño de los activos, gestión de configuraciones y detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Estas evaluaciones se llevarán a cabo cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de estos.
• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en este Anexo Técnico, 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 servicio correspondiente, así como herramientas en software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otros

disponibles). Estas cuentas serán de solo lectura, y sus atributos de consulta se definirán en las mesas establecidas para este propósito.
• Facilitar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licenciamiento adquirido para cada servicio proporcionado y otros datos relevantes para la toma de decisiones sobre el uso del servicio.
• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos DDoS para el análisis, depuración y mejor control de acceso y seguridad. Esta solución se implementará en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.
• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.4 Servicios de Redes Privadas Virtuales (VPN)
Descripción del servicio: Operbes S.A. de C.V., oferta y garantiza la continuidad operativa del servicio de interconexión a través de Internet, el cual posibilita establecer comunicaciones desde localidades remotas para la transferencia de información mediante un canal cifrado.

Por lo tanto, Operbes S.A. de C.V., oferta el cumplimiento de las siguientes especificaciones funcionales mínimas:
• Garantizar la continuidad operativa de los activos de infraestructura existentes en el Instituto, así como implementar los recursos necesarios para mantener esta continuidad, incluyendo soporte técnico, licenciamiento y cualquier otro requerimiento para cumplir con los niveles de servicio establecidos en el Apéndice B.
• Integrar activos de infraestructura específicos (Appliances) con capacidad de expansión según demanda, con el fin de asegurar la continuidad operativa del Instituto, conforme a lo especificado en el Apéndice A.
• Definir en colaboración con el Instituto la estrategia para asegurar la continuidad operativa de los activos de infraestructura actuales y futuros, de acuerdo con las necesidades operativas.
• Realizar las tareas necesarias para la instalación del equipo en los centros de datos correspondientes, o en cualquier otra ubicación requerida por el Instituto.
• Coordinar con el personal del Instituto, mediante el administrador del contrato o el modelo de gobierno designado, las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio. No se podrán realizar cambios en los componentes de hardware o software sin la autorización correspondiente.
• Proseguir con la integración de cada activo de infraestructura en su respectiva consola de administración centralizada, ya sea en modo independiente o stand alone, asegurando que la bitácora de cada activo esté integrada en la solución de correlación de eventos designada por el Instituto.
• Garantizar que los activos de infraestructura cuenten con actualizaciones tecnológicas del sistema operativo, aplicaciones (firmware) y otros componentes necesarios para su funcionamiento.
• Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.
• Continuar proporcionando acceso a los servicios ubicados en la capa de servidores de los centros de datos (DMZ), gestionando según el esquema de seguridad establecido 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 todas las solicitudes de cambio, incidentes, fallos y solicitudes de información generadas por el Instituto, siguiendo los Niveles de Servicio establecidos para tales fines.
• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura que conforman el servicio, cumpliendo al menos con lo siguiente:

- Notificar cualquier actividad sospechosa relacionada con la violación de las políticas, así como aquellas identificadas mediante las funcionalidades habilitadas en la solución.
- Informar sobre las fallas relacionadas con el hardware de los activos de infraestructura proporcionados a través del servicio.

•Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, incluyendo todas las renovaciones requeridas durante la duración de los servicios.

• Realizar evaluaciones operativas de los servicios, herramientas de software y activos de infraestructura, así como análisis de vulnerabilidades, con el fin de identificar mejoras en el rendimiento de los activos, en la gestión de configuraciones y en la detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Estas evaluaciones se llevarán a cabo cada 6 meses, desde el inicio de la operación de los servicios hasta 6 meses antes de su finalización.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en este Anexo Técnico, incluyendo componentes que faciliten las comunicaciones entre redes, el cableado eléctrico y de datos, el montaje en racks, entre otros.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas de software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otros disponibles), las cuales serán de solo lectura. Los atributos de consulta se definirán en las mesas integradas para este propósito.

• Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licenciamiento adquirido para cada servicio proporcionado, entre otros aspectos relevantes para la toma de decisiones sobre el uso del servicio.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos VPN para el análisis y depuración de estas, así como para mejorar el control de acceso y la seguridad. Esta solución se implementará en las instalaciones del centro de datos primario sin generar costos adicionales para el instituto.

• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.5 Servicios de Filtrado de Contenido Web

Descripción del servicio: Operbes S.A. de C.V., oferta y garantiza la continuidad operativa del servicio de filtrado de contenido web, el cual permite controlar y filtrar el acceso a Internet según roles y perfiles definidos.

En este sentido, Operbes S.A. de C.V., oferta el cumplimiento con las siguientes especificaciones funcionales mínimas:

• Garantizar la continuidad operativa de los activos de infraestructura actualmente en posesión del Instituto, así como la implementación de nuevos activos si fuera necesario. Esto incluye el soporte técnico, licenciamiento y cualquier otro requerimiento necesario para asegurar dicha continuidad operativa, todo de acuerdo con los niveles de servicio establecidos en el Apéndice B.

• Integrar activos de infraestructura específicos (Appliances) con capacidades de expansión bajo demanda para mantener la continuidad operativa del Instituto, conforme a lo establecido en el Apéndice A.

• Colaborar con el Instituto en la definición de la estrategia para habilitar la continuidad operativa de los activos de infraestructura actuales o los que se necesiten según los requisitos operativos.

• Realizar la instalación del equipo necesario en los Centros de Datos designados o en cualquier otra localidad requerida por el Instituto.

• Coordinar con el personal del Instituto, ya sea a través del administrador del contrato o el cuerpo de gobierno designado, las ventanas de mantenimiento necesarias para asegurar el correcto funcionamiento del servicio. No se

podrán realizar cambios en los componentes de hardware o software que integran el servicio sin la autorización correspondiente.

• Continuar integrando cada activo de infraestructura en su respectiva consola de administración centralizada, permitiendo la administración independiente (stand-alone) de los dispositivos, y asegurando que la bitácora de cada activo se integre adecuadamente en la solución de correlación de eventos del proyecto o en otra designada por el Instituto.

• Asegurar que los activos de infraestructura estén actualizados tecnológicamente, con un sistema operativo, aplicación (firmware) u otro componente necesario, estable y validado.

• Limitar el tráfico de datos únicamente al definido por el Instituto, tanto interno como externo, entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.

• Mantener el acceso a los servicios ubicados en la capa de servidores de los centros de datos (DMZ), gestionándolos de acuerdo con el esquema de seguridad establecido y respetando la segmentación definida entre las diferentes zonas de seguridad.

• Evitar la explotación de vulnerabilidades y el ingreso de tráfico malicioso a las redes del Instituto.

• Gestionar todos los requerimientos de cambio, incidentes/fallas y solicitudes de información generadas por el Instituto, siguiendo los Niveles de Servicio establecidos para dicho propósito.

• Monitorear todos los eventos registrados en la solución y emitir alertas sobre incidentes generados por los activos de infraestructura que integran el servicio, cumpliendo al menos con:

- Notificar actividades sospechosas relacionadas con la violación de políticas y aquellas identificadas mediante las funcionalidades habilitadas en la solución.
- Notificar sobre fallos relacionados con el hardware de los activos de infraestructura proporcionados a través del servicio.

• Integrar el licenciamiento del software necesario para mantener en funcionamiento los servicios y activos de infraestructura correspondientes, así como llevar a cabo todas las renovaciones requeridas durante la duración de los servicios.

• Realizar evaluaciones operativas a los servicios (herramientas de software y activos de infraestructura), así como análisis de vulnerabilidades, con el fin de identificar mejoras en el rendimiento de los activos, en la gestión de configuraciones, y detectar nuevas funcionalidades operativas derivadas de actualizaciones en las versiones de hardware y/o software. Estas evaluaciones se ejecutarán cada 6 meses, desde el inicio de las operaciones de los servicios hasta 6 meses antes de su finalización.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en la presente propuesta Técnica, como componentes que permitan la comunicación entre redes, el cableado eléctrico y de datos, el montaje en racks, entre otros.

• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas de software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otras disponibles). Estas cuentas serán de solo lectura, y los atributos de consulta se definirán en las mesas integradas para este propósito.

• Facilitar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para la solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licenciamiento adquirido para cada servicio proporcionado, y otros recursos que ayuden en la toma de decisiones sobre el uso del presente servicio.

• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos de Filtrado de Contenido Web para realizar análisis y depuración de estas, y mejorar el control de acceso y seguridad. Esta solución se implementará en las instalaciones del centro de datos primario sin incurrir en costos adicionales para el instituto.

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

iv.1.6 Servicios de Filtrado de Contenido de Correo (Antispam)
Descripción del servicio: Operbes S.A. de C.V., acepta y que que el Instituto busca garantizar la continuidad operativa de un servicio destinado al análisis de correos electrónicos de entrada y salida. Este servicio tiene como finalidad bloquear aquellos correos que sean identificados como spam, *malware*, *phishing*, o que contengan contenido malicioso, entre otros.

Por lo tanto, Operbes S.A. de C.V., oferta el cumplimiento de las siguientes especificaciones funcionales mínimas.
•Garantizar la continuidad operativa de los activos de infraestructura existentes en el Instituto, así como implementar nuevos recursos si es necesario. Esto incluye el soporte técnico, licenciamiento y cualquier otro requerimiento necesario para mantener la operatividad, de acuerdo con los niveles de servicio establecidos en el Apéndice B.
• Incorporar activos de infraestructura específicos (Appliances) con capacidad de expansión bajo demanda, según lo definido en el Apéndice A, para asegurar la continuidad operativa del Instituto.
• Trabajar en conjunto con el Instituto para definir la estrategia de habilitación que asegure la continuidad operativa de los activos de infraestructura actuales y futuros, según las necesidades operativas.
• Ejecutar todas las tareas necesarias para instalar el equipo en los Centros de Datos correspondientes, atendiendo las solicitudes del Instituto.
• Implementar un servicio de protección para el correo electrónico entrante y saliente, así como salvaguardar la reputación de las direcciones IP utilizadas para la comunicación en Internet, mediante un mecanismo de sanitización en la nube que brinde una doble capa de verificación sobre correos anómalos o no deseados.
• Establecer, en coordinación con el personal del Instituto, las ventanas de mantenimiento necesarias para la correcta operación del servicio, asegurando que cualquier cambio en los componentes de hardware o software esté autorizado.
• Mantener la integración de cada activo de infraestructura hacia su consola de administración centralizada, garantizando la integración de la bitácora de cada activo en la solución de correlación de eventos designada por el Instituto.
•Asegurar que los activos de infraestructura cuenten con actualizaciones tecnológicas del sistema operativo, aplicaciones (firmware) u otros componentes necesarios para su correcto funcionamiento.
• Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central y otros puntos de interconexión con redes externas.
• Continuar permitiendo el acceso a servicios ubicados en la capa de servidores de los centros de datos, gestionándolos según el esquema de seguridad establecido y respetando la segmentación entre las zonas de seguridad.
• Implementar medidas proactivas para evitar la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
• Brindar atención a todos los requerimientos de cambio, incidentes, fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos.
• Supervisar todos los eventos registrados en la solución y enviar alertas sobre incidentes generados por los activos de infraestructura del servicio, incluyendo notificaciones sobre actividades sospechosas y fallas de hardware.
- 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.

• Incluir el licenciamiento del software necesario para mantener los servicios y activos de infraestructura, así como realizar renovaciones durante la vigencia del contrato.

• Realizar evaluaciones periódicas de los servicios y activos de infraestructura para identificar mejoras y detectar nuevas funcionalidades operativas, así como analizar vulnerabilidades cada 6 meses.
• Implementar integraciones de conectividad física y lógica para habilitar los servicios descritos, incluyendo componentes como cableado, montaje en racks, entre otros.
• Facilitar al Instituto cuentas de acceso a las consolas de administración del servicio y a las bases de conocimiento de las tecnologías integradas, con información relevante para la toma de decisiones.
• Implementar un servicio de auditoría de reglas de acceso en dispositivos Antispam para mejorar el control de acceso y seguridad, sin costo adicional para el Instituto.
• Asegurar el cumplimiento de las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.7 Servicios de Firewall Especializado en Servicios Web (WAF)
Descripción del servicio. Operbes S.A. de C.V. oferta y garantiza la continuidad del servicio de protección, prevención y control de ataques dirigidos a los aplicativos *web* expuestos en Internet/Intranet.

Por ende, Operbes S.A. de C.V. oferta el cumplimiento de las siguientes especificaciones funcionales mínimas.
• Garantizar la continuidad operativa de los activos de infraestructura existentes en el Instituto, así como la implementación de cualquier recurso adicional necesario para mantener esta continuidad, lo que incluye soporte técnico, licenciamiento y cualquier otro requisito necesario para asegurar el servicio de acuerdo con lo estipulado en el Apéndice B.
• Integrar activos de infraestructura específicamente diseñados (Appliances) con capacidad de expansión bajo demanda, asegurando la continuidad operativa del Instituto según lo especificado en el Apéndice A.
• Colaborar con el Instituto para definir la estrategia de habilitación que asegure la continuidad operativa de los activos de infraestructura actuales y aquellos que sean necesarios para satisfacer las necesidades operativas.
• Realizar las tareas requeridas para instalar el equipo en los Centros de Datos correspondientes o en cualquier otra ubicación solicitada por el Instituto.
• Coordinar con el personal del Instituto, a través del administrador del contrato o del modelo de gobierno designado, las ventanas de mantenimiento necesarias para garantizar el correcto funcionamiento del servicio, asegurando que cualquier cambio en los componentes de hardware o software esté autorizado por el Instituto.
• Continuar integrando cada activo de infraestructura en su respectiva consola de administración centralizada, ya sea de forma independiente o en modo stand alone, asegurando que la bitácora de cada activo se integre en la solución de correlación de eventos designada por el Instituto.
• Garantizar la actualización tecnológica de los activos de infraestructura, incluyendo el sistema operativo, la aplicación (firmware) u otros componentes necesarios para el servicio correspondiente.
• Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.
• Mantener el acceso a los servicios en la capa de servidores de los centros de datos (DMZ), gestionándolos 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 en las redes del Instituto.
• Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información generados por el Instituto, cumpliendo con los Niveles de Servicio definidos para este propósito.
• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura que componen el servicio, notificando actividades sospechosas relacionadas con la violación de políticas o fallas en el hardware de los activos de infraestructura provistos a través del servicio.
- Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como realizar todas las renovaciones necesarias durante la vigencia de los servicios.

- Realizar evaluaciones operativas y análisis de vulnerabilidades de los servicios y activos de infraestructura para identificar mejoras en el desempeño, gestión de configuraciones y detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software, ejecutándose cada 6 meses desde el inicio de operaciones hasta 6 meses antes del término de estos.

• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en la propuesta Técnica, como componentes 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 servicio correspondiente, así como herramientas de software para acceder a las mismas, las cuales serán de solo lectura y cuyos atributos de consulta serán definidos en las mesas que se integren para este propósito.
• Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas, 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, entre otros aspectos relevantes para la toma de decisiones respecto al uso del servicio.
• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos WAF para analizar y depurar las mismas, mejorando el control de acceso y seguridad, con la solución implementada en las instalaciones del centro de datos primario sin costo adicional para el Instituto.
• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.8 Servicios de Firewall especializado en Base de Datos (DBF)

Descripción del servicio: Operbes S.A. de C.V. oferta mantener la operatividad continua del servicio de protección para las instancias de bases de datos en tiempo real, así como supervisar el tráfico de la base de datos para detectar ataques avanzados.

Por lo tanto, Operbes S.A. de C.V. oferta el cumplimiento de las las siguientes especificaciones funcionales mínimas.

•Garantizar la continuidad operativa de los activos de infraestructura del Instituto, ya sea los existentes o los que se necesiten implementar, proporcionando soporte técnico, licenciamiento y otros recursos necesarios para asegurar dicha continuidad, conforme a lo establecido en el Apéndice B.
• Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, según lo dispuesto en el Apéndice A, para mantener la continuidad operativa del Instituto.
• Definir en colaboración con el Instituto la estrategia de habilitación para mantener la continuidad operativa de los activos de infraestructura actuales o los que sean necesarios según las necesidades operativas.
• Realizar la instalación del equipo en los Centros de Datos correspondientes o en otras ubicaciones solicitadas por el Instituto.
• Acordar con el personal del Instituto, ya sea a través del administrador del contrato o el modelo de gobierno designado, las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio, y abstenerse de realizar cambios en los componentes de hardware o software sin una autorización de cambio previa.
• Continuar integrando cada activo de infraestructura en su respectiva consola de administración centralizada, ya sea en modo stand-alone para la administración de todos los dispositivos o mediante otras configuraciones requeridas, garantizando la integración de las bitácoras de cada activo en la solución de correlación de eventos definida por el Instituto.
• Garantizar la actualización tecnológica de los activos de infraestructura, incluyendo el sistema operativo, aplicación (firmware) y otros componentes necesarios.
• Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.
• Mantener el acceso a los servicios ubicados en la capa de servidores de los centros de datos (Base de datos), gestionando según el esquema de seguridad y respetando la segmentación definida entre las zonas de servidores.

• Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
• Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información generados por el Instituto, cumpliendo con los Niveles de Servicio definidos.
• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura del servicio, notificando sobre actividades sospechosas relacionadas con la violación de las políticas y fallas relacionadas con el hardware de los activos de infraestructura.
  - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
• Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura correspondientes, así como realizar todas las renovaciones necesarias durante la vigencia de los servicios.
• Realizar evaluaciones operativas y análisis de vulnerabilidades a los servicios y activos de infraestructura cada 6 meses, desde el inicio de operaciones hasta 6 meses antes del término de estos, identificando mejoras en el desempeño, gestión de configuraciones y nuevas funcionalidades operativas.
• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en la presente propuesta Técnica, 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 servicio, así como herramientas en software que permitan acceder a las mismas, garantizando que sean de solo lectura y definiendo los atributos de consulta en las mesas correspondientes.
• Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas, donde se pueda consultar información sobre casos de soporte, documentación técnica, pólizas de mantenimiento vigentes, licenciamiento adquirido, y otras que faciliten la toma de decisiones.
• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos DBF para mejorar el control de acceso y seguridad, implementado en las instalaciones del centro de datos primario sin costo adicional para el Instituto.
• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.9 Servicios de Gestión Unificada de Amenazas (UTM)
Descripción del servicio: Operbes S.A. de C.V., acepta que el Instituto busca asegurar la continuidad operativa del servicio de protección perimetral especializado en control de acceso, prevención de intrusos, filtrado de contenido web y VPN, con el fin de controlar el tráfico y detectar actividades anómalas.

Por lo tanto, Operbes S.A. de C.V. oferta el cumplimiento de las siguientes especificaciones funcionales mínimas.
• Garantizar la continuidad operativa de los activos de infraestructura existentes en el Instituto o implementar nuevos activos según sea necesario. Esto incluye proporcionar soporte técnico, licenciamiento y cualquier otro requisito para garantizar esta continuidad operativa, en conformidad con lo establecido en el Apéndice B.
• Integrar activos de infraestructura específicos (Appliances) con capacidad de expansión bajo demanda para mantener la continuidad operativa del Instituto, de acuerdo con lo estipulado en el Apéndice A.
• Definir en colaboración con el Instituto la estrategia para habilitar la continuidad operativa de los activos de infraestructura actuales o los nuevos requeridos para satisfacer las necesidades operativas.
• Realizar todas las tareas necesarias para instalar el equipo en los Centros de Datos correspondientes, o en cualquier otra ubicación solicitada por el Instituto.

• Acordar con el personal del Instituto, a través del administrador del contrato o el modelo de gobierno designado, las ventanas de mantenimiento necesarias para garantizar el correcto funcionamiento del servicio, asegurando que cualquier cambio en los componentes de hardware o software del servicio sea autorizado mediante un control de cambios.
• Continuar integrando cada activo de infraestructura en su consola de administración centralizada respectiva, ya sea en modo independiente o en conjunto, y asegurar que el registro de cada activo esté integrado en la solución de correlación de eventos especificada por el Instituto.
• Garantizar que los activos de infraestructura estén actualizados tecnológicamente, incluyendo el sistema operativo, la aplicación (firmware) u otros componentes necesarios para el servicio correspondiente.
• Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes.
• Prevenir la explotación de vulnerabilidades y el ingreso de tráfico malicioso a las redes del Instituto.
• Atender todos los requerimientos de cambio, incidentes/fallas y solicitudes de información generados por el Instituto, en conformidad con los Niveles de Servicio definidos.
• Monitorear todos los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura que componen el servicio, notificando actividades sospechosas relacionadas con violaciones de políticas y fallas en hardware.
  - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
• Integrar el licenciamiento del software necesario para mantener los servicios y activos de infraestructura, incluyendo todas las renovaciones requeridas durante la vigencia de los servicios.
• Realizar evaluaciones operativas y análisis de vulnerabilidades a los servicios y activos de infraestructura cada seis meses, identificando mejoras en el desempeño, la gestión de configuraciones y la detección de nuevas funcionalidades operativas.
• Realizar las integraciones de conectividad física y lógica necesarias para habilitar los servicios descritos en la presente Propuesta Técnica, como componentes de comunicación entre redes, cableado eléctrico y de datos, y montaje en racks.
• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio correspondiente, así como herramientas de software para acceder a las mismas, con atributos de consulta definidos en mesas de trabajo específicas.
• Proporcionar al Instituto acceso a bases de conocimiento de las tecnologías integradas, donde se pueda consultar información sobre casos de soporte, documentación técnica, pólizas de mantenimiento y licenciamiento adquirido para cada servicio proporcionado.
• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos UTM para análisis, depuración y mejor control de acceso y seguridad, sin generar costo adicional para el Instituto.
• Cumplir con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.10 Servicio de Correlación de Eventos
Descripción del servicio: Operbes S.A. de C.V., eferta un servicio de seguridad que gestione, analice, explote, utilice y aproveche los registros de actividad de los dispositivos de seguridad para comprender completamente lo que sucede en varios puntos de la red de manera centralizada y eliminar los falsos positivos generados.

Por lo tanto, Operbes S.A. de C.V., oferta el cumplimiento de las siguientes especificaciones funcionales mínimas.

• Proveer activos de infraestructura de última generación, exclusivamente dedicados a satisfacer las necesidades del Instituto.
• Habilitar los activos de infraestructura en esquemas de Alta Disponibilidad (HA).
• Integrar activos de infraestructura de propósito específico (appliances o servidores físicos) con capacidades de expansión bajo demanda, pudiendo estas últimas ser instancias virtuales, según lo dispuesto en el Apéndice A.
• Definir en colaboración con el Instituto la estrategia para habilitar los nuevos activos de infraestructura para la correlación de eventos en la arquitectura de seguridad y comunicaciones.
• Ejecutar todas las tareas necesarias para instalar el equipo en los Centros de Datos correspondientes, o en cualquier otra ubicación requerida por el Instituto.
• Coordinar con el personal del Instituto, a través del administrador del contrato o el modelo de gobierno designado, todas las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio. No se realizarán cambios a los componentes de hardware/software sin un control de cambios autorizado por el Instituto.
• Integrar cada activo de infraestructura en su respectiva consola de administración centralizada, ya sea en modo independiente (stand alone) para la administración de todos los dispositivos, asegurando que la bitácora de cada activo esté integrada en la solución de correlación de eventos del proyecto o en otra designada por el Instituto.
• Garantizar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada del sistema operativo, aplicación (firmware) u otro componente necesario.
• Permitir únicamente la correlación definida por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión vía syslog con otras redes o nubes.
• Atender los requerimientos de cambio, atención de fallas y solicitudes de información generadas por el Instituto, según los Niveles de Servicio definidos.
• Monitorear los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura del servicio, notificando actividades sospechosas relacionadas con la violación de las políticas y fallas de hardware.

- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
- Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

• En caso de rendimiento inadecuado, presentar propuestas de mejora de los activos afectados y sustituir componentes tecnológicos por otros de igual o mejores características/funcionalidades, con autorización previa del Instituto.
• Integrar el licenciamiento del software necesario para habilitar los servicios y activos de infraestructura correspondientes, así como realizar renovaciones durante la vigencia de los servicios.
• Realizar evaluaciones operativas cada 6 meses para identificar mejoras en el desempeño de los activos, gestión de configuraciones y detección de nuevas funcionalidades, derivadas de actualizaciones en versiones de hardware y/o software.
• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio y herramientas en software de solo lectura, cuyos atributos de consulta se definirán en mesas específicas.
• Proporcionar al Instituto cuentas de acceso a bases de conocimiento de las tecnologías integradas para la solución, incluyendo información sobre casos de soporte, documentación técnica, pólizas de mantenimiento y licenciamiento adquirido.
• Incluir un servicio de auditoría de reglas de acceso en los dispositivos del Correlacionador de Eventos para análisis, depuración y mejor control de acceso y seguridad, implementado en las instalaciones del centro de datos primario sin costo adicional para el Instituto.
• Cumplir, como mínimo, con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.1.11 Servicio de Protección de Amenazas Persistentes Avanzadas (APT)
Descripción del servicio: Operbes S.A. de C.V., acepta que Instituto busca implementar un servicio que le brinde la capacidad de protegerse contra amenazas avanzadas que puedan estar activas dentro de la organización y que hayan eludido los controles de seguridad existentes.

En este sentido, Operbes S.A. de C.V., oferta el cumplimiento de las siguientes especificaciones funcionales mínimas.
• Proveer activos de infraestructura de última generación, dedicados exclusivamente a las necesidades del Instituto.
• Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA).
• Integrar activos de infraestructura de propósito específico (appliances) con capacidades de expansión bajo demanda, pudiendo estas últimas ser instancias virtuales, según lo dispuesto en el Apéndice A.
• Definir en colaboración con el Instituto la estrategia para habilitar los nuevos activos de infraestructura para la detección de Amenazas Persistentes Avanzadas en la arquitectura de seguridad y comunicaciones.
• Ejecutar las tareas necesarias para la instalación del equipo en los Centros de Datos correspondientes, o en cualquier otra ubicación solicitada por el Instituto.
• Coordinar con el personal del Instituto, a través del administrador del contrato o el cuerpo de gobierno designado, todas las ventanas de mantenimiento necesarias para el correcto funcionamiento del servicio, sin realizar cambios a los componentes de hardware/software sin autorización.
• Integrar cada activo de infraestructura en su respectiva consola de administración centralizada, asegurando que la bitácora de cada activo quede integrada en la solución de correlación de eventos designada por el Instituto.
• Garantizar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada del sistema operativo, aplicación (firmware) u otro componente necesario.
• Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central y los diferentes puntos de interconexión con otras redes o nubes, previniendo la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
• Atender los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información generadas por el Instituto, apegado a los Niveles de Servicio definidos.
• Monitorear los eventos registrados en la solución y emitir alertas de incidentes generados por los activos de infraestructura del servicio, notificando actividades sospechosas relacionadas con la violación de las políticas y fallas de hardware.
  - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
• En caso de rendimiento inadecuado, presentar propuestas de mejora de los activos afectados y sustituir componentes tecnológicos por otros de igual o mejores características/funcionalidades, con autorización previa del Instituto.
• Integrar el licenciamiento del software necesario para habilitar los servicios y activos de infraestructura correspondientes, así como realizar renovaciones durante la vigencia de los servicios.
• Realizar evaluaciones operativas cada 6 meses para identificar mejoras en el desempeño de los activos, gestión de configuraciones y detección de nuevas funcionalidades, derivadas de actualizaciones en versiones de hardware y/o software.
• Proporcionar al Instituto cuentas de acceso a las consolas de administración del servicio y herramientas en software de solo lectura, cuyos atributos de consulta se definirán en mesas específicas.

• Proporcionar al Instituto cuentas de acceso a bases de conocimiento de las tecnologías integradas para la solución, incluyendo información sobre casos de soporte, documentación técnica, pólizas de mantenimiento y licenciamiento adquirido.
• Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos del servicio de Amenazas Persistentes Avanzadas para análisis, depuración y mejor control de acceso y seguridad, implementado en las instalaciones del centro de datos primario sin costo adicional para el Instituto.
• Cumplir, como mínimo, con las especificaciones técnicas y operativas descritas en el Apéndice A.

iv.2 Servicios de Seguridad – Verificación y Calidad
Operbes S.A. de C.V., poferta mantener la prestación de servicios bajo demanda durante la vigencia del contrato, con el objetivo de definir, identificar, clasificar y priorizar las debilidades de las aplicaciones que proporcionan una evaluación de las amenazas previsibles. Esto permitirá reaccionar de manera adecuada y fortalecer la confidencialidad, integridad y disponibilidad de la información, en línea con las necesidades operativas del IMSS.

iv.2.1 Servicios de Borrado Seguro de Información
Descripción del servicio: Operbes S.A. de C.V., oferta y se compromente a mantener la solución de borrado seguro de información para una variedad de dispositivos, incluyendo computadoras personales, laptops, servidores, unidades de almacenamiento fijas y removibles, así como cualquier otro dispositivo determinado por el Instituto. El objetivo es evitar la pérdida y dispersión de información propiedad del Instituto cuando estos dispositivos sean retirados debido a razones como la conclusión de contratos, obsolescencia, fallas, bajas o reasignaciones, entre otros motivos. Para lograrlo, es necesario renovar el derecho de uso y soporte técnico de los productos de software de borrado seguro, así como actualizar el licenciamiento correspondiente. Estas actualizaciones (updates y upgrades) garantizarán la confidencialidad de la información del Instituto, cumpliendo con la legislación vigente sobre derechos de autor.

Operbes S.A. de C.V., oferta el cumplimiento de las siguientes especificaciones funcionales mínimas y asegurar que los servicios y entregas de información estén de conformidad con la normativa aplicable para dichas soluciones y servicios.
• Integrar todas las renovaciones 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.
• Permitir la realización de borrados completos en medios de almacenamiento dispuestos en activos de infraestructura como equipos de cómputo (de escritorio y portátiles), equipos de propósito específico (appliance), servidores físicos o virtuales, derivado de la sustitución, migraciones o retiro por finalización del contrato.
• 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, tanto de estado sólido como mecánicos, independientemente de su tamaño.
• Destrucción local y/o remota en múltiples dispositivos de almacenamiento.
• Capacidades para desmontar RAID (SCSI) cuando sea necesario.
• Facilitación del proceso de borrado y detección de zonas bloqueadas/ocultas (DCO, HPA).

ANEXOS
DIVISIÓN DE CONTRATOS

• Generación de certificados de borrado infalsificables, incluyendo el resultado del proceso de borrado, fecha, hora, detalles del equipo y del dispositivo de almacenamiento borrado, con el fin de ofrecer protección legal.
• Emisión de una firma electrónica para autenticar la integridad del reporte de sanitización emitido por el software de borrado.
• Ejecución de la solución sin importar el sistema operativo utilizado.
• Exportación del reporte generado por la solución a un medio de almacenamiento como USB o disco duro.
• El servicio de borrado seguro se proporciona a través de un proceso operativo que incluye:
- Solicitud de borrado.
- Identificación del medio a borrar.
- Definición de fecha para el borrado.
- Flujos operativos para autorización de borrado o destrucción.
- Se muestran los insumos a ser atendidos como referencia.

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

Operbes S.A. de C.V., ofera y acepta que es fundamental que la continuidad del servicio garantice que los usuarios tengan acceso a las consolas de administración de la solución. Esto les permitirá gestionar, administrar, supervisar y operar, con el objetivo de habilitar las funcionalidades necesarias para llevar a cabo el borrado seguro de manera descentralizada, incluso en oficinas remotas.

iv.2.2 Servicio de Gestión de Dominios
Descripción del servicio: Garantizar la continuidad operativa para el registro y gestión de dominios conforme a los requisitos establecidos por el NIC. Operbes S.A. de C.V., oferta el cumplimiento de las con las siguientes especificaciones funcionales mínimas:

• Registro:
- Seguimiento ante las instancias certificadoras.
- Coordinación con el personal designado por el Instituto para el nombre de dominio acordado.
- Verificación de la no duplicación o uso por terceros del nombre de dominio.
• Alojamiento:
- Supervisión del alojamiento del dominio.
- Actualización de las directivas de seguridad.

- Mantenimiento continuo según sea necesario.

Operbes S.A. de C.V. oferta y será responsable de la gestión y los pagos relacionados con el registro, cambio de dominio o proveedor, sin costos adicionales para el Instituto.

iv.2.3 Servicio de Certificados Digitales SSL

Descripción del Servicio: Operbes S.A. de C.V., oferta y acepta que se busca garantizar la continuidad del servicio para obtener certificados SSL destinados a proteger las páginas web del Instituto durante la duración del contrato. Por lo tanto, Operbes S.A. de C.V., oferta el cumplimiento de las con las siguientes especificaciones funcionales mínimas:

• Validación de dominios.
• Encripción SSL de al menos 256 bits.
• Los certificados no serán auto firmados, sino emitidos por instancias certificadoras válidas (terceros de confianza).
• El tiempo de emisión cumplirá con los niveles de servicio establecidos para su entrega al personal del Instituto vía correo electrónico.
• Operbes S.A. de C.V. se encargará de la gestión de los pagos de derechos y cualquier otro cargo asociado a la obtención y mantenimiento de los certificados.
• Los certificados serán, al menos, de los siguientes tipos:
  - Certificados SSL con validación de dominio (DV SSL):
  - Certificado para un solo dominio.
  - Certificado para múltiples dominios (SAN).
  - Certificados comodines (wildcard).
  - Certificados para código.

iv.2.4 Servicios de Ciberinteligencia (Ciberseguridad)

Descripción del servicio: Operbes S.A. de C.V., oferta y acepta que el Instituto busca un servicio de inteligencia con capacidad de acción que le permita responder de manera oportuna ante amenazas o ataques informáticos detectados a través de campañas y operaciones identificadas, así como realizar investigaciones según sus necesidades.

Por lo tanto, Operbes S.A. de C.V., oferta el cumplimiento de las siguientes especificaciones funcionales mínimas:

• Detección de posible venta de información confidencial del Instituto en mercado negro.
• Seguimiento de grupos hacktivistas y del cibercrimen nacionales y extranjeros que representen una amenaza para el Instituto.
• Infiltración en canales de IRC donde se organicen y difundan campañas de ataques informáticos que puedan afectar al Instituto.
• Monitoreo de foros y comunidades en redes abiertas y en la Red Onion/Tor donde se perpetren y difundan campañas de ataques informáticos que representen un riesgo para el Instituto.
• Vigilancia de noticias nacionales y extranjeras en la red abierta y en la Deep web para recopilar inteligencia táctica que permita al Instituto tomar acciones preventivas adicionales para proteger su infraestructura de posibles ataques informáticos.
• Recopilación de información a través de un cuestionario especializado para realizar el análisis de la situación global del Instituto y generar perfiles de investigación para los servicios permanentes.
  - Páginas publicadas.
  - Historial de amenazas de seguridad experimentadas por el Instituto.
  - Sistemas críticos consultados por usuarios externos.
  - Lista de activos críticos y su atracción o valor para el ciber-crimen.
  - Contactos para la elaboración de la matriz de escalación.
  - Datos para la elaboración de la declaración de trabajo (SOW por sus siglas en inglés).

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

• Análisis de la situación global del Instituto teniendo en cuenta el contexto del entorno y la identificación de exposiciones y amenazas que podrían impactarle, tanto a nivel local como global.
• Generación de perfiles de investigación con la información recabada, incluyendo perfiles virtuales a emplear y definición de fuentes asociadas a los perfiles virtuales utilizados en el monitoreo.
- Perfiles virtuales para emplear.
- Definición de fuentes asociadas a los perfiles virtuales utilizados en el monitoreo.

• Establecimiento de umbrales para eventos que desencadenarán alertas hacia la matriz de notificación definida en conjunto con el Instituto para los servicios de "Vigilancia Permanente de Ciberinteligencia".
• Mantenimiento de supervisión de correos/sitios de phishing y direcciones IP sospechosas proporcionadas por el Instituto para su análisis. Además, se llevará a cabo vigilancia continua en el ciberespacio las 24 horas del día, los 365 días del año, incluyendo redes sociales, Darknet y buscadores de Internet de las cosas. Se utilizarán técnicas de OSINT (Inteligencia de Fuentes Abiertas) como líneas de tiempo y mapas de conexiones, así como Virtual HUMINT para la infiltración de perfiles virtuales.
• Identificación de campañas para ataques específicos, venta de información y exposición de infraestructura vulnerable en Internet, así como relaciones entre perfiles y grupos privados de Facebook, entre otros.
• Realización de evaluaciones en los siguientes casos:
- Durante la vigilancia de Ciberinteligencia al identificar una amenaza real para el Instituto.
- Cuando se solicite análisis de sitios o correos de phishing, o direcciones IP.
- Durante análisis de grupos hacktivistas.
- Durante análisis de direcciones IP de ataques de denegación de servicio experimentados por el Instituto.

• Realizar un análisis correlacionando información recolectada con eventos específicos y emisión de dictámenes con inteligencia accionable hacia el Instituto en un plazo máximo de 24 horas después de la detección de eventos críticos, como ataques de denegación de servicio, defacements, fuga de información, phishing, entre otros.
- Declaración de posibles ataques de denegación de servicio por parte de grupos hacktivistas o del cibercrimen.
- Defacements.
- Fuga de información confidencial del Instituto hacia sitios públicos.
- Malware dirigido.
- Phishing detectado en parking domains.
- Indicios de amenazas o ataques informáticos sobre el Instituto.
- Existencia de campañas (conjunto de acciones para perpetrar un ataque informático) en contra del Instituto.
- Venta o publicación de información sensible del Instituto en la Darknet.
- Publicación de información confidencial de personal del Instituto como usuarios y contraseñas.
- Nuevos esquemas de fraude detectados en otros organismos del sector.

• Generación de procesos de inteligencia accionable en casos donde se haya detectado un ataque con impacto en el Instituto o en análisis a petición del Instituto sobre phishing y direcciones IP, proporcionando recomendaciones pertinentes.
- Cuando se detecte que un ataque ya sucedió y tuvo un impacto en el Instituto, para lo cual se emitirán recomendaciones hacia el Instituto.
- En los casos donde se realice el análisis a petición del Instituto de sitios o correos relacionados con phishing así como direcciones IP, se generará a partir de los hallazgos identificados inteligencia accionable donde se incluirá detalles sobre los sitios, direcciones IP, artefactos maliciosos, entre otros, al igual que sobre los reportes generados como parte de los servicios.

• Análisis mensual de direcciones IP sospechosas para identificar posibles actividades de ataque, intrusiones a otros organismos similares, participación en botnets, defacements u otras campañas específicas.

• Análisis del hacktivismo en México, incluyendo operaciones actuales, objetivos e impacto, proporcionando recomendaciones de protección.
• Análisis de correos electrónicos o sitios web sospechosos, incluyendo identificación de encabezados, análisis de *malware*, extracción de datos y evaluación de riesgo en una plataforma de Inteligencia sobre Amenazas.
- Identificación de los encabezados y análisis del *malware* en el contenido.
- Extracción de datos como dominios y direcciones IP, mismas que serán analizadas en una plataforma de "Inteligencia sobre Amenazas" para determinar el riesgo que representa el Phishing para el Instituto.

iv.2.5 Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos Móviles.
Descripción del servicio: Operbes S.A. de C.V. oferta un serviciode protección en redes inalámbricas específicas que permitan colocar controles que garanticen y protejan la información producida internamente y recibida a través de los recursos de redes inalámbricas (WLAN), contra ataques generales que buscan aprovechar esta modalidad para infiltrarse en la red de comunicaciones del Instituto, así mismo se considera un servicio de protección de dispositivos móviles, que prevenga el robo o sustracción de información considerando para lo anterior, la administración de políticas y el cumplimiento de operación en los dispositivos móviles.

Por lo que Operbes S.A. de C.V., oferta el cumplimiento de las siguientes especificaciones funcionales mínimas.
• Garantizar que las herramientas propuestas para el servicio cuenten con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios con el que cuente el servicio correspondiente.
• Integrar el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
• Proteger contra ataques informáticos comunes a la red inalámbrica (WLAN).
• Actualizar y mejorar los procesos que permitan la autenticación de usuarios internos.
• Cifrado TKIP y AES basado en hardware.
• Tener la funcionalidad de WIPS en tiempo real (prevención de intrusiones inalámbricas).
• Integrado en un tercer radio de banda doble específico (sin afectar el rendimiento del punto de acceso).
• Permitir aplicar políticas de control sobre las aplicaciones que los dispositivos
• Permitir la instalación de aplicaciones y ejecutar actualizaciones en múltiples dispositivos a la vez de manera remota y controlando el tipo de conexión y la fecha de ejecución.
• Permitir realizar modificaciones de cambio de contraseña de bloqueo, y también se puede configurar la longitud, el tipo de contraseña, si es alfanumérica o numérica, el número de intentos, entre otros.
• Permitir a los administradores del sistema mantener y controlar estos dispositivos de forma centralizada.
• Analizar los dispositivos para asegurarse de que cumplen con la política del Instituto.
• Recuperar toda la información sobre los dispositivos, incluidos los detalles del dispositivo, certificados, aplicaciones instaladas, entre otros.
• Regular el acceso a las cuentas Institucionales tales como cuentas de correo electrónico, Wi-Fi y VPN.
• Bloquear los dispositivos de forma remota para evitar robados o perdida de información.
• Soportará la conexión desde dispositivos móviles y de escritorio a través de un cliente de acceso remoto. Dicho cliente soportará al menos las siguientes plataformas operativas: MAC OS X, iOS, Android, Windows desde v7.
• Alarmas.

iv.2.6 Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA).
Descripción del servicio: Operbes S.A. de C.V., oferta un servicio de control de acceso para usuarios privilegiados con el objetivo de brindar funcionalidades de control y monitoreo de las cuentas de usuarios privilegiados en sus

servidores, así como implementar un sistema de Autenticación, Autorización y Contabilización (AAA, por sus siglas en inglés: Authentication, Authorization and Accounting).

Por lo tanto, Operbes S.A. de C.V., oferta el cumplimiento de las siguientes especificaciones funcionales mínimas:

- Implementar una solución tecnológica que permita un control detallado del acceso a los activos de infraestructura que respaldan las aplicaciones, mediante la administración del ciclo de vida de las identidades.
- Integrar procesos que identifiquen los roles y perfiles de cada usuario por aplicación, junto con la capacidad de rastrear los accesos realizados, incluyendo la captura de imágenes de pantalla y la grabación de video de las sesiones de acceso.
- Considerar, entre otras, las siguientes plataformas operativas:
  - Microsoft Windows
  - Unix
  - Linux
- Revisar y validar junto con el Instituto los requisitos para proteger las claves privilegiadas en los servidores donde se implementará el servicio.
- Implementar los agentes proporcionados por la solución en los sistemas operativos respaldados por los fabricantes correspondientes.
- Llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona de los Centros de Datos designados por el Instituto.
- Acordar con el personal del Instituto las ventanas de mantenimiento necesarias según el tiempo de implementación requerido.
- Integrar el dispositivo con la consola de administración de la solución y garantizar la integración de la bitácora del dispositivo con la solución de Correlación del proyecto.
- Ofrecer servicios de autenticación, autorización y registro (AAA) para habilitar el control de acceso e identidad en la red del Instituto.
- Habilitar los activos de infraestructura necesarios en esquemas de Alta Disponibilidad (HA).
- Capacidad para generar políticas basadas en reglas y atributos.
- Integración con bases de datos externas como Active Directory y LDAP.
- Capacidad de integrarse con un dominio de Directorio Activo.
- Integración con soluciones de contraseña única.
- Integración con dispositivos de red para aplicar políticas de seguridad basadas en identidad.
- Utilización de los siguientes protocolos de autenticación:
  - CHAP/MSCHAP
  - PAP
  - PEAP
  - EAP-TLS
  - MS-CHAP
  - EAP-MD5
- Generación de políticas de restricción por dispositivo y horario.
- Uso de listas de acceso descargables.
- Capacidad para operar en esquemas de clúster con más de 3 dispositivos funcionando como un solo sistema.
- Funcionalidad para operar en esquemas de procesamiento físico (appliance) o virtualizados.
- Interfaz de administración gráfica basada en web.

• Interfaz de programación para operaciones de actualización, creación, lectura y eliminación de dispositivos, terminales y usuarios en la base de datos interna.
• Funcionalidades de reporte y auditoría.
• Capacidades de monitoreo y diagnóstico de problemas.
• Administración de eventos (logs) exportables.

iv.2.7 Servicio de Antivirus

Operbes S.A. de C.V. oferta preveer el licenciamiento, instalación, habilitación, configuración, puesta a punto, gestión, monitoreo, soporte y mantenimiento de una solución diseñada para proteger contra amenazas de código malicioso que puedan afectar a los dispositivos de trabajo, servidores, correos electrónicos externos e internos, así como la navegación web hacia Internet. Además, se aplicarán políticas de seguridad con el objetivo de fortalecer los controles para mitigar riesgos, proteger la infraestructura institucional y garantizar la continuidad operativa de las actividades de los usuarios.

La protección antivirus se llevará a cabo mediante un agente distribuido a los activos de infraestructura requeridos por el Instituto. Operbes S.A. de C.V., oferta y se compromente a asegurar la entrega de dicho agente a los activos de infraestructura especificados por el Instituto. La distribución y administración del agente puede llevarse a cabo tanto en entornos locales (on-premise) como en la nube.

Operbes S.A. de C.V., oferta realizar las actividades de remediación de infecciones por virus serán de su responsabilidad. Por lo tanto, brindará el apoyo necesario mediante la utilización de las funcionalidades proporcionadas por la solución antivirus propuesta como parte del servicio actual. Además, Operbes S.A. de C.V. notificará al personal designado por el Instituto sobre cualquier actividad sospechosa detectada, ya sea a través de correo electrónico u otro medio acordado por ambas partes. Asimismo, se ocupará de atender los incidentes de *malware* según lo estipulado en los Acuerdos de Nivel de Servicio o los Acuerdos de Nivel Operativo.

En el caso de que la instalación requerida por el Instituto supere los 200 agentes, Operbes S.A. de C.V. , en colaboración con el Instituto, establecerá una estrategia para implementar el agente antivirus y garantizará la actualización de este en todos los activos de infraestructura solicitados, sin que ello afecte el funcionamiento del Instituto. Es importante considerar que estos activos y consolas de administración podrán estar distribuidos en diferentes localidades del Instituto.

Operbes S.A. de C.V. configurará las políticas de seguridad base en la solución antivirus propuesta, las cuales se definirán en conjunto con el Instituto como parte de las reglas que regirán el servicio. Estas políticas serán desplegadas en los activos de infraestructura correspondientes a través de la consola de administración de la solución. Además, Operbes S.A. de C.V. ajustará estas políticas según sea necesario, basándose en el monitoreo continuo de la solución y en los requerimientos del Instituto.

Operbes S.A. de C.V. oferta y acepta que se requerirá que entre Operbes S.A. de C.V. y el Instituto definan una estrategia para la entrega de actualizaciones de antivirus en todos los activos de infraestructura, asegurando que no se vean afectadas las operaciones de los servicios internos, los cuales están distribuidos en diferentes localidades a nivel nacional. Operbes S.A. de C.V. oferta y se compromente a mantener actualizados en todo momento los activos de infraestructura con la última versión o actualización de antivirus proporcionada por el fabricante.

ANEXOS
DIVISIÓN DE CONTRATOS

Además, Operbes S.A. de C.V. , en colaboración con el Instituto, determinará la cantidad de activos de infraestructura que constituirán la línea base para el primer año de prestación del servicio. Posteriormente, un mes antes de cumplir cada año de servicio, se llevará a cabo una redefinición de esta línea base para el próximo año.

Operbes S.A. de C.V. suministrará al personal del Instituto la última versión del agente de antivirus para su integración en la imagen de software de los Puestos de Servicio.

Como parte de la operación del presente servicio, Operbes S.A. de C.V:
•Emitirá alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Antivirus.
•Monitoreará el cumplimiento de las políticas de uso de información implantadas en la solución.
•Notificará sobre las actividades sospechosas relacionadas con la infección de activos de infraestructura.
•Notificará sobre todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la Solución de Antivirus, efectuando la contención de estas a través de la solución propuesta.
•Resolverá las solicitudes de soporte técnico especializado, a fin de evitar y prevenir infecciones en los activos de infraestructura donde se encuentre instalada la solución de Antivirus.
•Recolectará e integrará, al menos la información de eventos de seguridad o logs generada por la solución de Antivirus, hacia la solución de correlación de eventos, cuyo detalle de información a integrar será definido entre el Instituto y Operbes S.A. de C.V.
•Desarrollará la afinación de la solución con base en el resultado del monitoreo continuo, además de gestionar las reglas antivirus en los activos de infraestructura, con base en las necesidades del Instituto y en el resultado del monitoreo día a día.

iv.2.8 Servicios de Prevención de Pérdida de Información
Descripción del servicio: Operbes S.A. de C.V., oferta una solución para detectar y prevenir la fuga y/o pérdida de información sensible en los activos de infraestructura del IMSS ubicados en los Centros de Datos. Esta solución estará integrada con los activos de infraestructura, el servicio de correo electrónico externo, el correo electrónico interno, la navegación web y los portales de colaboración, lo que permitirá una visión completa y una prevención efectiva en múltiples capas de seguridad.
El módulo tendrá la capacidad de establecer políticas mediante el uso de palabras clave o expresiones regulares que identifiquen información sensible, bloqueando su transmisión a través de diferentes canales de comunicación.
El servicio se enfocará en prevenir la fuga de información sensible desde los puestos de servicio.
Operbes S.A. de C.V. configurará en la solución propuesta las políticas base de seguridad definidas en colaboración con el Instituto, adaptándolas a los activos de infraestructura y creando los perfiles correspondientes.

Estas políticas se desplegarán a través de la consola de administración de la solución, y Operbes S.A. de C.V. será responsable de ajustarlas mediante un proceso de puesta a punto continuo, basado en su monitoreo constante y los requisitos específicos del Instituto. Para este fin, Operbes S.A. de C.V., oferta al menos, las siguientes premisas:
• **Tipos de documentos:** Este apartado incluye las diversas formas en que se pueden estructurar los activos de información relevantes para los procesos del Instituto. Incluyen, entre otros, reportes, estudios, oficios, correspondencia, acuerdos, directivas, planes estratégicos, contratos, convenios, anotaciones, memorandos, estadísticas, procedimientos, políticas, reglamentos, informes, solicitudes, encuestas, históricos y otros documentos similares.
• **Medios de almacenamiento de la información:** Este apartado hace referencia a los diferentes medios disponibles para resguardar los activos de información con el propósito de manipularlos en el futuro.

Operbes S.A. de C.V. garantizará que las funcionalidades de la Solución de Prevención de Pérdida de Información se cumplan incluso si el activo de infraestructura no está asociado a ningún Directorio Activo o a la red del Instituto.
En el marco de la operación del servicio, Operbes S.A. de C.V:

- Emitirá alertas de incidentes y vigilar los eventos generados por los componentes tecnológicos de la solución de Prevención de Pérdida de Información.
- Supervisará el cumplimiento de las políticas de uso de la información establecidas en la solución.
- Informará al Instituto sobre actividades sospechosas relacionadas con la violación de las políticas de fuga de información configuradas en los activos de infraestructura.
- Implementará medidas de contención ante actividades sospechosas.
- Atenderá las solicitudes de soporte técnico especializado para prevenir fugas de información en los equipos donde esté habilitada la solución.
- Recopilará e integrará, al menos, la información de eventos de seguridad o registros generados por la solución de Prevención de Pérdida de Información en la solución de correlación de eventos, cuyo alcance será definido entre el Instituto y Operbes S.A. de C.V..
- Gestionará los componentes tecnológicos a través de procesos de gestión de cambios, configuraciones y versiones según los requisitos del Instituto.

La solución propuesta por Operbes S.A. de C.V. contará con las siguientes funcionalidades:

- Presentará un registro de auditoría que contenga todas las actividades realizadas por los usuarios.
- Ofrecerá reportes predefinidos y personalizados que puedan ser programados o generados de manera puntual.
- Disponerá de un mecanismo de alertas y notificaciones.
- Tecnología de Detección:
  - Capacidad para extraer texto de diversos tipos de documentos para llevar a cabo análisis de contenido.
  - Habilidad para realizar detecciones basadas en palabras clave o frases clave personalizadas, con la capacidad de combinar múltiples palabras en una sola regla de detección.
- Capacidad para realizar análisis de contenido en varios canales de información (correo electrónico, HTTPS/HTTP, FTP, entre otros).

iv.2.9 Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)

Operbes S.A. de C.V. oferta y acepta que el servicio tiene como objetivo asegurar la continuidad operativa del Sistema de Gestión de Seguridad de la Información (SGSI), el cual estará alineado con el estándar ISO/IEC 27001:2022. Este sistema se encargará de emitir directivas relacionadas con la seguridad de la información tanto a las áreas de TI como a los terceros responsables de apoyar la operación de TI. Es fundamental que este servicio sea adaptable a las actualizaciones necesarias para mantener la conformidad con las últimas versiones y requisitos normativos.

Operbes S.A. de C.V. oferta y aceota garantizar el cumplimiento de las la continuidad operativa del mismo, ofreciendo al menos las siguientes funcionalidades operativas:

Planificación:

Capacitación de seguimiento: Se llevará a cabo un curso de "Inducción a la norma ISO/IEC 27001:2022 o la versión vigente", con el objetivo de proporcionar a los participantes las habilidades necesarias para:

- Comprender la estructura de la norma ISO/IEC 27001:2022.
- Interpretar los requisitos necesarios para el cumplimiento de dicha norma.
- Conocer las etapas fundamentales para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).
- Se contempla la participación de al menos 8 personas, con una duración mínima de 8 horas y máxima de 40 horas.

Seguimiento y actualización en la aplicación de las directivas en materia de seguridad: Revisión y actualización del Manual de Políticas de Seguridad de la Información que cumplirá con los siguientes criterios:

- Cubrir los dominios establecidos por la norma ISO/IEC 27001:2022.
- Incluir los procesos de seguridad aplicables según la normativa actual.
- Estar dirigido tanto a las áreas de TI como a los terceros que prestan servicios de TI al Instituto, abordando al menos 20 directivas relacionadas con el catálogo de infraestructuras críticas del Instituto.

Identificación y evaluación de activos (relacionados con el catálogo de infraestructuras críticas) del proceso involucrado en el Sistema de Gestión de Seguridad de la Información.

La metodología que seguirá contempla los siguientes aspectos:

- Identificación de los activos del proceso.
- Valoración de los activos del proceso.
- Identificación de los requisitos de seguridad.
- Identificación de los controles de seguridad existentes.

Generación de la Declaración de Aplicabilidad (SoA: Statement of Applicability).

La metodología abordará los siguientes aspectos:

- Identificación y evaluación de la aplicabilidad de los requerimientos internos y externos.
- Selección de los objetivos de control y los controles para mitigar los riesgos.
- Verificación de los requisitos contractuales y legales.
- Identificación de los requisitos internos y externos pertinentes.
- Validación de la aplicabilidad de los requisitos identificados.
- Elaboración del Formato de Autorización para la implementación y operación del Sistema de Gestión de Seguridad de la Información.
- Preparación de la Declaración de Aplicabilidad.
- Documentación de los objetivos de control, los controles seleccionados y la justificación de su elección.
- Documentación de los controles actualmente implementados.
- Documentación de la exclusión de controles y la justificación de dicha exclusión.

Operación del Sistema de Gestión de Seguridad de la Información

- Análisis de Riesgos de Seguridad de la Información
- Análisis de riesgos basado en el servicio definido de gestión de riesgos de seguridad.
- Generación y actualización del plan de tratamiento de riesgos.

La metodología considera los siguientes aspectos:

- Identificación de las acciones a realizar por parte de la institución y su administración.
- Identificación de los recursos necesarios y establecimiento de prioridades.
- Asignación de responsabilidades para la gestión de riesgos de seguridad de la información.

Aplicación del seguimiento al plan de tratamiento de riesgos.

La metodología considera los siguientes aspectos:

- Asignación de roles y responsabilidades para supervisar los controles relacionados con personas, procesos y tecnología involucrados en la mitigación de los riesgos.
- Actualización de la documentación, conforme 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 abordará los siguientes temas:

- Control de accesos.

- Monitoreo de cuentas.
- Definición del proceso de Continuidad del Negocio.
- Implementación de los roles y responsabilidades definidos para el Sistema de Gestión de Seguridad de la Información.
- Controles de seguridad en la infraestructura tecnológica, conforme a lo establecido en el alcance.

Gestión del cambio cultural.

La metodología abordará los siguientes aspectos:

- Actualización del Programa de Concientización dirigido a usuarios y operadores del Sistema de Gestión de Seguridad de la Información.
- Seguimiento y apoyo a las necesidades de capacitación del personal encargado de administrar el Sistema de Gestión de Seguridad de la Información y de la seguridad de la información.
- Elaboración o actualización del Manual de Gestión de Seguridad de la Información. Este manual incluirá las referencias generadas en esta fase para garantizar la trazabilidad de las cláusulas de la norma.

Monitoreo y revisión del Sistema de Gestión de Seguridad de la Información.

La metodología abordará los siguientes aspectos:

- Los responsables del proceso realizarán una revisión y actualización del Sistema de Gestión de Seguridad de la Información para garantizar que los objetivos de este sistema estén alineados con los objetivos de negocio en materia de seguridad de la información, y que aseguren el manejo adecuado de los riesgos existentes.
- Operbes S.A. de C.V. actualizará el procedimiento de las revisiones gerenciales.
- Asimismo, Operbes S.A. de C.V. actualizará los formatos necesarios para llevar a cabo las revisiones gerenciales.

Auditorías internas.

La metodología incluye lo siguiente:

- Seguimiento y apoyo en la elaboración del plan de auditorías internas para las áreas de TI y para los terceros que proporcionan servicios de TI al Instituto.
- Actualización o, en su caso, definición de los formatos necesarios para llevar a cabo las auditorías.
- Ejecución de una auditoría interna del Sistema de Gestión de Seguridad de la Información para verificar el cumplimiento con el estándar ISO/IEC 27001:2022 o la normativa vigente, así como con los procesos establecidos en la normativa aplicable.

Actualización del Sistema de Gestión de Seguridad de la Información e Implementación de Mejoras

Considerará los siguientes aspectos:

- Priorización de las acciones correctivas y de las no conformidades identificadas en las revisiones gerenciales, revisiones independientes, auditorías internas y revisiones técnicas.
- Identificación de los responsables encargados de llevar a cabo las mejoras.
- El Instituto establecerá fechas de compromiso para la finalización de las mejoras, exclusivamente para seguimiento interno.

Acciones Correctivas y No Conformidades

Operbes S.A. de C.V., oferta lo siguiente:

- Apoyo en la definición y seguimiento del procedimiento para llevar a cabo acciones correctivas y atender no conformidades derivadas de las auditorías.
- Actualización del formato para el registro de acciones correctivas y no conformidades.
- Coordinación de la ejecución de las acciones correctivas ya definidas y, en caso necesario, de las no conformidades identificadas.

Comunicación de los Resultados de las Acciones Tomadas

ANEXOS
DIVISIÓN DE CONTRATOS

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

Operbes S.A. de C.V., oferta los siguientes puntos:

- Apoyo en la programación de reuniones de seguimiento al Sistema de Gestión de Seguridad de la Información, con el fin de informar sobre el alcance de las acciones correctivas y las no conformidades abordadas, y verificar su cumplimiento con los requisitos de los propietarios de la información y de los involucrados en los procesos del Instituto.

iv.2.10 Servicios Continuidad de Gestión del Cambio en Seguridad de la Información
Descripción del Servicio: Operbes S.A. de C.V., oferta la implementación de un programa de gestión del cambio para fortalecer la protección de la información, en consonancia con los requisitos del estándar ISO/IEC 27001:2022, mediante una estrategia cultural.

Este servicio incluirá un plan exhaustivo de transferencia de conocimientos al personal del Instituto sobre los principales aspectos de seguridad de la información, incluyendo al menos los siguientes ámbitos:

- Regulación actual en materia de seguridad de la información.
- Políticas de seguridad específicas del Instituto.
- Procesos relacionados con la seguridad en el Instituto.
- Controles de seguridad implementados en el Instituto.

El servicio se estructura en las siguientes etapas:

Etapa 1: Definición de la Estrategia de Gestión del Cambio

- Contextualización del Instituto: Operbes S.A. de C.V. comprenderá el contexto cultural del Instituto en lo que respecta a la seguridad de la información.
- Diagnóstico del Estado Actual: Operbes S.A. de C.V. realizará un análisis para evaluar el nivel de conocimiento existente en seguridad de la información, identificando las brechas entre la situación actual y los requisitos establecidos por el Instituto.
- Preparación de la Estrategia: Basándose en los resultados del diagnóstico, Operbes S.A. de C.V. propondrá una estrategia de gestión del cambio en seguridad de la información para facilitar una transferencia efectiva de conocimientos.

Etapa 2: Diseño del Programa de Gestión del Cambio

- Preparación del Programa: Operbes S.A. de C.V., oferta elaborar un plan de trabajo detallado que incluirá los temas a abordar en la transferencia de conocimientos, el número de personal involucrado y las fechas de implementación.
- Elaboración de Contenidos: Operbes S.A. de C.V., oferta desarrollar materiales en formato PowerPoint u otros definidos por el Instituto, que serán utilizados para la transferencia de conocimientos en seguridad de la información.
- Creación del Modelo de Evaluación: Operbes S.A. de C.V., oferta presentar un modelo de evaluación destinado a medir la efectividad de la transferencia de conocimientos en seguridad de la información.
- Preparación del Grupo de "Train the Trainers": Operbes S.A. de C.V., identificará y preparará a un grupo de 5 facilitadores con el fin de que puedan replicar la transferencia de conocimientos en otras áreas clave dentro del Instituto.

Etapa 3: Comunicación del Programa de Gestión del Cambio

- Implementación de la Transferencia: Operbes S.A. de C.V., ejecutará la transferencia de conocimientos al personal de Tecnologías de la Información del Instituto y a las áreas definidas por este, ubicadas en la Ciudad de México.

Etapa 4: Medición del Programa de Gestión del Cambio

- Implementación de Evaluaciones: Operbes S.A. de C.V. pondrá en marcha una herramienta tecnológica para realizar evaluaciones en línea a los participantes de la transferencia de conocimientos.
- Análisis de Datos: Operbes S.A. de C.V. analizará la información recopilada para organizar los resultados obtenidos.
- Presentación de Resultados: Operbes S.A. de C.V. llevará a cabo una presentación ejecutiva ante el personal de Tecnologías de la Información del Instituto, en la que se expondrán los resultados generales obtenidos.

iv.2.10 Servicios del Centro de Operaciones de Seguridad (SOC)

Operbes S.A. de C.V. cuenta con un Centro de Operaciones de Seguridad (SOC) que esté físicamente ubicado en las instalaciones de Operbes S.A. de C.V. El propósito de este centro será garantizar la continuidad operativa y gestionar la seguridad, así como encargarse de la administración, operación, monitoreo, soporte y resolución de fallas de los componentes de las soluciones de seguridad. Esto implica llevar a cabo actividades como revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, y establecimiento de acciones para mejorar de manera sostenible.

El servicio del Centro Operaciones de Seguridad (SOC), que respaldará la operación y prestación del servicio requerido por el Instituto ofrecerá un control continuo, mayor eficiencia y oportunidad de mejora. Para lograr esto, Operbes S.A. de C.V. proporcionará servicios de tecnología de la información confiables en lo que respecta a la gestión de servicios de TI. Estos servicios estarán respaldados por certificaciones ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018 vigentes y emitidas a nombre de Operbes, S.A. de C.V:

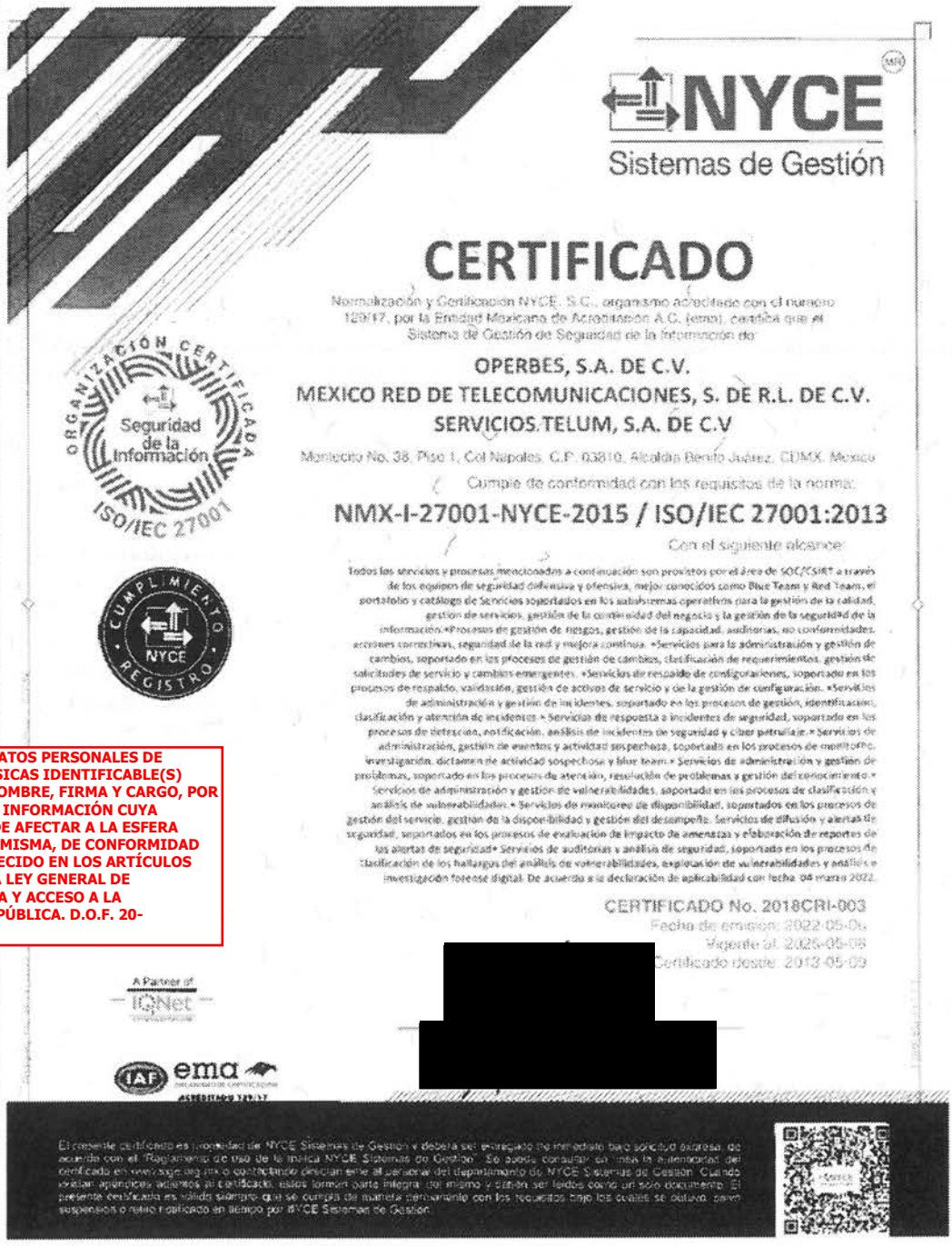
Operbes S.A. de C.V. tendrá en cuenta que el servicio de SOC se refiere a las soluciones propuestas e implementadas actualmente por el instituto. Además, considerará que la correlación de bitácoras se basará en un servicio de correlación de eventos e incidentes de seguridad en el que los casos de uso serán ilimitados. Asimismo, las respuestas a incidentes estarán alineadas con los niveles de servicio (SLA) establecidos para este servicio, garantizando tiempos de respuesta adecuados.

El Centro de Operaciones de Seguridad (SOC) estará ubicado en el territorio nacional, lo cual se puede verificar con una copia simple de las certificaciones ISO/IEC27001:2022 e ISO/IEC20000-1:2018 a nombre de Operbes S.A. de C.V. participante.

A continuación se presenta copia de las certificaciones correspondientes.

ANEXOS
DIVISIÓN DE CONTRATOS

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025



NYCE
Sistemas de Gestión

CERTIFICADO

Normalización y Certificación NYCE, S.C., organismo acreditado con el número 129/17, por la Entidad Mexicana de Acreditación A.C. (ema), certifica que el Sistema de Gestión de Seguridad de la Información de

OPERBES, S.A. DE C.V.
MEXICO RED DE TELECOMUNICACIONES, S. DE R.L. DE C.V.
SERVICIOS TELUM, S.A. DE C.V

Manlecito No. 38, Piso 1, Col Napoles, C.P. 03810, Alcaldía Benito Juárez, CDMX, Mexico

Cumple de conformidad con los requisitos de la norma:

NMX-I-27001-NYCE-2015 / ISO/IEC 27001:2013

Con el siguiente alcance:

Todos los servicios y procesos mencionados a continuación son provistos por el área de SOC/CSIRT a través de los equipos de seguridad defensiva y ofensiva, mejor conocidos como Blue Team y Red Team, el portafolio y catálogo de Servicios soportados en los subsistemas operativos para la gestión de la calidad, gestión de servicios, gestión de la continuidad del negocio y la gestión de la seguridad de la información.•Procesos de gestión de riesgos, gestión de la capacidad, auditorías, no conformidades, acciones correctivas, seguridad de la red y mejora continua. •Servicios para la administración y gestión de cambios, soportado en los procesos de gestión de cambios, clasificación de requerimientos, gestión de solicitudes de servicio y cambios emergentes. •Servicios de respaldo de configuraciones, soportado en los procesos de respaldo, validación, gestión de activos de servicio y de la gestión de configuración. •Servicios de administración y gestión de los identes, soportado en los procesos de gestión, identificación, clasificación y atención de incidentes. • Servicios de respuesta a incidentes de seguridad, soportado en los procesos de detección, notificación, análisis de incidentes de seguridad y cibar petrullaje.• Servicios de administración, gestión de eventos y actividad sospechosa, soportado en los procesos de monitoreo, investigación, dictamen de actividad sospechosa y blue team.• Servicios de administración y gestión de problemas, soportado en los procesos de atención, resolución de problemas y gestión del conocimiento.• Servicios de administración y gestión de vulnerabilidades, soportado en los procesos de clasificación y análisis de vulnerabilidades. • Servicios de monitoreo de disponibilidad, soportados en los procesos de gestión del servicio, gestión de la disponibilidad y gestión del desempeño. Servicios de difusión y alertas de seguridad, soportados en los procesos de evaluación de impacto de amenazas y elaboración de reportes de las alertas de seguridad• Servicios de auditorías y análisis de seguridad, soportado en los procesos de clasificación de los hallazgos del análisis de vulnerabilidades, explotación de vulnerabilidades y análisis e investigación forense digital. De acuerdo a la declaración de aplicabilidad con fecha 04 marzo 2022.

CERTIFICADO No. 2018CRI-003
Fecha de emisión: 2022-05-06
Vigente al: 2025-05-08
Certificado desde: 2013-05-09

[redacted]

El presente certificado es propiedad de NYCE Sistemas de Gestión y deberá ser entregado inmediato bajo solicitud expresa, de acuerdo con el "Reglamento de uso de la marca NYCE Sistemas de Gestión". Se puede consultar en línea la autenticidad del certificado en www.nyce.org.mx o contactando directamente al personal del departamento de NYCE Sistemas de Gestión. Cuando existan apéndices adjuntos al certificado, estos forman parte integral del mismo y deben ser leídos como un solo documento. El presente certificado es válido siempre que se cumpla de manera permanente con los requisitos bajo los cuales se otorgó, salvo suspensión o retiro notificado en tiempo por NYCE Sistemas de Gestión.

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: NOMBRE, FIRMA Y CARGO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

IQNet

THE INTERNATIONAL CERTIFICATION NETWORK

CERTIFICATE

Normalización y Certificación NYCE, S.C. has issued an IQNet recognized certificate that the organization:

OPERBES, S.A. DE C.V.
MEXICO RED DE TELECOMUNICACIONES, S. DE R.L. DE C.V.
SERVICIOS TELUM, S.A. DE C.V

Headquarter: Montecito No. 38, Piso 1, Col Nápoles, C.P. 03810, Benito Juárez, CDMX. México

has implemented and maintains a

Information Security Management System

for the following scope:

All the services and processes mentioned below are provided by the SOC / CSIRT area through the defensive and offensive security teams, better known as Blue Team and Red Team, the portfolio and catalog of Services supported in the operational subsystems for the quality management, service management, business continuity management and information security management: • Risk management processes, capacity management, audits, non-conformities, corrective actions, network security and continuous improvement. • Services for the administration and management of changes, supported in the processes of change management, requirements classification, service request management and emerging changes. • Configuration backup services, supported in the backup, validation, service asset management and configuration management processes. • Incident management and administration services, supported in the processes of management, identification, classification and attention to incidents • Security incident response services, supported in the detection, notification, analysis of security incidents and cyber patrol processes. • Administration services, management of events and suspicious activity, supported in the processes of monitoring, investigation, opinion of suspicious activity and blue team. • Administration and management services of problems, supported in the processes of attention, problem solving and knowledge management • Vulnerability management and administration services, supported in the vulnerability analysis and classification processes • Availability monitoring services, supported in the service management, availability management and performance management processes. Dissemination services and security alerts, supported in the processes for evaluating the impact of threats and preparing reports on security alerts. • Security auditing and analysis services, supported in the processes of classifying the findings of the vulnerability analysis, vulnerability exploitation and digital forensic analysis and investigation. According to the Applicability Statement dated March 04, 2022.

which fulfils the requirements of the following standard

ISO/IEC 27001:2013

Issued on: **2022-05-06**
Expires on: **2025-05-08**
First Issued: **2013-05-09**

This attestation is directly linked to the IQNet Partner's original certificate and shall not be used as a stand-alone document

Registration Number: **MX- 2018CRI-003**

[redacted]

NYCE Sistemas de Gestión

IQNet Partners*:
AENOR Spain AFNOR Certification France APCER Portugal CCC Cyprus CISQ Italy
CQC China CQM China CQS Czech Republic Cro Cert Croatia DQS Holding GmbH Germany EAGLE Certification Group USA
FCAV Brazil FONDONORMA Venezuela ICONTEC Colombia Inspecta Sertifointi Oy Finland INTECO Costa Rica
IRAM Argentina JQA Japan KFQ Korea MIRTEC Greece MSZT Hungary Nemko AS Norway NSAI Ireland
NYCE-SIGE México PCBC Poland Quality Austria Austria RR Russia SII Israel SIQ Slovenia
SIRIM QAS International Malaysia SQS Switzerland SRAC Romania TEST St Petersburg Russia TSE Turkey YUQS Serbia

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: NOMBRE, FIRMA Y CARGO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

ANEXOS
DIVISIÓN DE CONTRATOS

NYCE
Sistemas de Gestión

CERTIFICADO

Normalización y Certificación NYCE, S.C., organismo acreditado con el número 129/17, por la Entidad Mexicana de Acreditación A.C. (ema), certifica que el Sistema de Gestión de Servicios de

OPERBES, S.A. DE C.V.
MEXICO RED DE TELECOMUNICACIONES, S. A. DE R.L. DE C.V.
SERVICIOS TELUM, S.A. DE C.V.

Montecito No. 38, Piso 1, Col Nápoles, C.P. 03810, Alcaldía Benito Juárez, CDMX, México.
Cumple de conformidad con los requisitos de la norma

NMX-I-20000-1-NYCE-2019 / ISO/IEC 20000-1:2018

Con el siguiente alcance:

Todos los servicios y procesos mencionados a continuación son provistos por el área de SOC/CSIRT a través de los equipos de seguridad defensiva y ofensiva, mejor conocidos como Blue Team y Red Team, el portafolio y catálogo de Servicios soportados en los subsistemas operativos para la gestión de la calidad, gestión de servicios, gestión de la continuidad del negocio y la gestión de la seguridad de la información:•Procesos de gestión de riesgos, gestión de la capacidad, auditorías, no conformidades, acciones correctivas, seguridad de la red y mejora continua. •Servicios para la administración y gestión de cambios, soportado en los procesos de gestión de cambios, clasificación de requerimientos, gestión de solicitudes de servicio y cambios emergentes. •Servicios de respaldo de configuraciones, soportado en los procesos de respaldo, validación, gestión de activos de servicio y de la gestión de configuración. •Servicios de administración y gestión de incidentes, soportado en los procesos de gestión, identificación, clasificación y atención de incidentes.• Servicios de respuesta a incidentes de seguridad, soportado en los procesos de detección, notificación, análisis de incidentes de seguridad y ciber patrullaje.• Servicios de administración, gestión de eventos y actividad sospechosa, soportado en los procesos de monitoreo, investigación, dictamen de actividad sospechosa y blue team. • Servicios de administración y gestión de problemas, soportado en los procesos de atención, resolución de problemas y gestión del conocimiento. • Servicios de administración y gestión de vulnerabilidades, soportado en los procesos de clasificación y análisis de vulnerabilidades. • Servicios de monitoreo de disponibilidad, soportados en los procesos de gestión del servicio, gestión de la disponibilidad y gestión del desempeño. Servicios de difusión y alertas de seguridad, soportados en los procesos de evaluación de impacto de amenazas y elaboración de reportes de las alertas de seguridad• Servicios de auditorías y análisis de seguridad, soportado en los procesos de clasificación de los hallazgos del análisis de vulnerabilidades, explotación de vulnerabilidades y análisis e investigación forense digital. De acuerdo a la declaración de aplicabilidad con fecha 04 marzo 2022.

[redacted]

FICADO No. 2018CRC-007
ha de emisión: 2022-05-09
Vigente al: 2025-05-09
rtificado desde: 2013-05-09

[redacted]

A Partner of IQNet

ema
ORGANISMO DE CERTIFICACIÓN
ACREDITADO 129/17

El presente certificado es propiedad de NYCE Sistemas de Gestión y deberá ser entregado de inmediato bajo solicitud expresa, de acuerdo con el Reglamento de uso de la marca NYCE Sistemas de Gestión. Se puede consultar en línea la autenticidad del certificado en www.sige.org.mx o contactando directamente al personal del departamento de NYCE Sistemas de Gestión. Cuando existan anexos adjuntos al certificado, estos forman parte integral del mismo y deben ser leídos como un solo documento. El presente certificado es válido siempre que se cumpla de manera permanente con los requisitos bajo los cuales se obtuvo, salvo suspensión o retiro notificado en tiempo por NYCE Sistemas de Gestión.

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: NOMBRE, FIRMA Y CARGO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

Este SOC cumplirá con las siguientes especificaciones:

- Funcionamiento continuo las 24 horas del día, los 7 días de la semana, los 365 días del año (7x24x365), de acuerdo con lo establecido en el contrato.
- Disponibilidad de personal cualificado para brindar atención tanto en el lugar como de forma remota, con las credenciales necesarias para administrar y monitorear los componentes de la solución.
- Operación en un centro de datos alternativo ubicado en el territorio nacional.
- Mantenimiento de suscripciones a sitios y listas de empresas, fabricantes y medios especializados en seguridad de la información para detectar nuevas vulnerabilidades.
- Infraestructura dedicada para la gestión, operación y monitoreo de los componentes de hardware y software de los servicios de seguridad.
- Ejecución de evaluaciones operativas a los servicios (software y activos de infraestructura) cada 3 meses desde el inicio de operaciones y hasta 3 meses antes de la finalización de estos, con el fin de identificar mejoras en el rendimiento, la gestión de configuraciones y nuevas funcionalidades.
- Implementación de acciones correctivas y preventivas para garantizar la confidencialidad, integridad y disponibilidad de la información manejada en las soluciones de seguridad.
- Envío de notificaciones y alertas personalizadas en caso de desviaciones, anomalías o brechas de seguridad para cada solución de seguridad.
- Revisiones continuas de la operación del SOC para mejorar procesos, procedimientos y controles de seguridad.
- Análisis de eventos de seguridad y registros de administración integrados en los servicios de correlación de información para establecer acciones preventivas mediante modificaciones en las configuraciones de las soluciones de seguridad.
- Integración de un Equipo de Atención y Respuesta a Incidentes de Seguridad.
- Soporte y atención a fallas de los componentes de hardware y software de la solución según lo establecido en los acuerdos de niveles de servicio.
- Monitoreo de la disponibilidad de los componentes hardware y software de la solución, con capacidad para generar alertas y notificaciones en caso de fallos, degradación del rendimiento, intermitencia o pérdida de disponibilidad.
- Mantenimiento preventivo y correctivo de las soluciones de seguridad habilitadas y los activos de infraestructura que respaldan cada servicio.
- Ejecutar procesos operativos para al menos los siguientes rubros:
    - Gestión de Riesgos
    - Gestión de Continuidad
    - Monitoreo y Detección
    - Gestión de Seguridad de la información
    - Administración de Dispositivos
    - Gestión de solicitudes de servicio
    - Administración de Cambios Operacionales
    - Administración de Configuraciones
    - Administración de Vulnerabilidades
    - Gestión de Incidentes
    - Gestión de Problemas

• Integración de una Mesa de Servicio conforme a las prácticas de ITIL v4, la cual será compatible con la Mesa de Servicios Tecnológicos del Instituto. Esta integración incluirá todas las actividades relacionadas con la configuración,

ANEXOS
DIVISIÓN DE CONTRATOS

desarrollo de software, ajustes, y otras tareas necesarias para facilitar la comunicación y el intercambio de requerimientos, cambios, incidentes y otros procesos determinados por el Instituto.

• El servicio de gestión de requerimientos, cambios, incidentes y otras solicitudes permitirá la creación de eventos (tickets) a través de los mecanismos definidos en las mesas de trabajo correspondientes, los cuales incluyen, de manera ejemplificativa pero no limitativa:

- Un número telefónico directo en las instalaciones del SOC.
- Un número telefónico de diez dígitos.
- Correo electrónico.
- Portal web.

• El Instituto se reserva el derecho de solicitar la revisión de la infraestructura de seguridad por un tercero en cualquier momento durante la vigencia del contrato, con el fin de asegurar la entrega adecuada del servicio.

• Supervisión de la Base de Datos de la Gestión de la Configuración (CMDB, por sus siglas en inglés), la cual contendrá los detalles pertinentes de cada elemento de configuración (CI) y sus relaciones, incluyendo equipos físicos, software, y las interconexiones entre incidencias, problemas, cambios y demás datos del servicio de seguridad.

• Generación de informes de Inteligencia de Negocios y Análisis de Información para obtener estadísticas sobre el uso y rendimiento de los servicios de seguridad. Esto tiene como objetivo respaldar la toma de decisiones estratégicas y operativas, así como determinar el plan de capacidad para cada tecnología implementada. Estos informes pueden incluir, entre otros datos, lo siguiente:

- Estadísticas de utilización de procesamiento por tecnología.
- Estadísticas de rendimiento por tecnología (throughput).
- Estadísticas de ataques informáticos bloqueados.
- Estadísticas de comportamientos típicos esperados por tecnología (líneas base).
- Estadísticas de usuarios concurrentes por servicio.
- Estadísticas de crecimiento diario y mensual para cada servicio.

• Facilitar al Instituto cuentas de acceso a las consolas de administración de los servicios de seguridad, así como proporcionar herramientas de software que permitan acceder a estas consolas (ya sea mediante aplicaciones cliente-servidor, portales web u otros medios disponibles). Estas cuentas tendrán únicamente permisos de lectura, y los atributos de consulta se definirán en las reuniones establecidas con ese fin.

• Las consolas de administración proporcionadas para los servicios de seguridad permitirán visualizar, como mínimo:

- 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. Estas bases de datos contendrán información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimiento vigentes, licencias adquiridas para cada servicio proporcionado, y cualquier otra información relevante que facilite la toma de decisiones con respecto al uso de los servicios de seguridad.

• Implementar un Tablero de Estadísticas de Servicios de Seguridad a través de un portal único de administración de los servicios de seguridad, independiente de las consolas de administración y herramientas de monitoreo. Este tablero proporcionará información estratégica en tiempo real y de manera histórica sobre el uso de los servicios, permitiendo al Instituto obtener una visión general del rendimiento de las soluciones, su estado de salud, incidentes registrados,

reportes de actividades sospechosas relevantes a nivel mundial, u otra información pertinente para la toma de decisiones sobre las condiciones operativas de los servicios. Operbes S.A. de C.V. incluirá en su oferta económica los costos asociados al desarrollo para cumplir con este requisito.

• Habilitar al personal designado por el administrador del contrato para generar reportes haciendo uso de todas las variables y funcionalidades de la herramienta de monitoreo. Se proporcionará la opción de parametrizar estos reportes y acceder a ellos a través de una interfaz web.

V. Perfil de Operbes S.A. de C.V.

Operbes S.A. de C.V. demostra la capacidad y competencia técnica certificada para implementar y operar soluciones de seguridad, asegurando su correcto funcionamiento en los sitios requeridos por "EL INSTITUTO". Para cumplir con este requisito, Operbes, S.A. de C.V. entrega una copia simple del acta constitutiva que acredite al menos cinco años de actividad empresarial en el rubro de proveeduría de servicios de seguridad de la información o áreas relacionadas, de acuerdo con las características y especificaciones establecidas en el presente Anexo Técnico.

El personal responsable de las operaciones de los servicios de seguridad contará con experiencia demostrada en tecnología y seguridad de la información. Para cumplir con este requisito Operbes, S.A. de C.V. entregará de los currículos vitae de todos los recursos humanos involucrados en el servicio, los cuales incluirán al menos:

- Experiencia profesional: Se evaluarán todos los puestos anteriores de cada miembro del equipo, detallando las fechas, nombres de los empleadores, títulos de los puestos y las responsabilidades asociadas. Se exigirá una experiencia mínima comprobada de tres años.
- Experiencia en proyectos especializados en Seguridad de la Información: Se mencionarán y describirán todos los proyectos en los que el personal haya participado, con una experiencia comprobada mínima de tres años en esta área.
- Estudios: Se registrarán todos los estudios relacionados con la seguridad de la información, así como las certificaciones vigentes a la fecha de presentación de la propuesta técnica. Se requerirán certificaciones de tecnología y/o seguridad de tipo "vendor-neutral".
- Estructura del equipo de trabajo: Se proporcionará una descripción de la estructura del grupo de trabajo, detallando las responsabilidades y competencias de cada perfil.
- Los servicios ofrecidos por el o los licitantes estarán respaldados por certificaciones ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018 vigentes. Incluidas en la presente propuesta.

Operbes, S.A. de C.V. entrega una copia simple del acta constitutiva que acredite al menos cinco años de actividad empresarial en el rubro de proveeduría de servicios de seguridad de la información o áreas relacionadas y las certificaciones ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018 vigentes. Incluidas en la presente propuesta.

A continuación, se enumeran las credenciales y capacidades que cumplirán los recursos asignados al proyecto:

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

Partida 1.

Perfil	Certificaciones que Operbes,S.A. de C.V. entregará	Experiencia que se demostrará	Función	Número de recursos
Administrador del Centro de Operaciones de Seguridad (SOC)	CISM (Certified Information Security Manager) o CISSP (Certified Information Systems Security Professional)	Tres años de experiencia en proyectos relacionados con seguridad de la información.	Responsable de la administración, monitoreo y operación de los servicios provistos por el SOC, además de brindar soporte y atención a fallas e incidentes de seguridad.	Al menos 1
Administración y Operación de soluciones y herramientas tecnológicas	Especialista consultor en cada una de las soluciones de seguridad integradas. Se aceptan como documentos comprobables los certificados vigentes obtenidos directamente del fabricante.	Tres años de experiencia en proyectos relacionados con seguridad de la información.	Administrar, operar y monitorear las soluciones de seguridad propuestas.	Al menos 1 por cada servicio
Líder de proyecto	PMP (Project Manager Professional) Certificado por PMI o ITIL v4 (Expert o Master)	Tres años de experiencia en proyectos relacionados con seguridad de la información.	Responsable de administrar y coordinar el proyecto	Al menos 2
Operador de la mesa de servicios SOC	ITIL v4 Foundation Certification	Tres años de experiencia participando en proyectos de seguridad de la información.	Personal encargado de las operaciones de soporte de primer nivel, monitoreo de servicios, registro y seguimiento de solicitudes de ventanas de mantenimiento, reporte de fallas y requerimientos.	Al menos 8
Arquitecto especializado en redes y seguridad.	CCNP (Cisco Certified Network Professional)	Tres años de experiencia en participación en proyectos de redes y seguridad de la información.	Responsable de la administración, monitoreo y operación de los servicios proporcionados por el SOC en lo referente a servicios de interconexión de red, así como del soporte y la atención a fallas e incidentes que surjan en la interoperabilidad con otros proveedores y/o fabricantes.	Al menos 1

VI. Condiciones técnicas de aceptación de entregable

Durante la habilitación, transición y operación de los servicios de seguridad, Operbes S.A. de C.V., oferta proporcionar diversos tipos de documentos, informes, artefactos, dictámenes o esquemas que aseguren el buen desempeño y continuidad del servicio. Estos documentos proporcionarán certeza sobre las actividades diarias que Operbes S.A. de C.V. llevará a cabo bajo la supervisión de los servidores públicos designados por el Instituto para este propósito.

Entregables Generales

Partida 1.

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto	Única Vez	15 días naturales posteriores a la emisión del fallo
	Documento Compromiso de suscripción del acuerdo de niveles operacional (*Operational Level Agreement*, OLA)	Única Vez	15 días naturales posteriores a la emisión del fallo
	Matriz de Escalación	Única Vez	15 días naturales posteriores a la emisión del fallo
	Escrito por parte de Operbes S.A. de C.V., firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	Única Vez	15 días naturales posteriores a la emisión del fallo
Servicios de Seguridad – Continuidad Operativa	Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel 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 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

ANEXOS
DIVISIÓN DE CONTRATOS

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Borrado Seguro de Información	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicio de Gestión de Dominios	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicio de Certificados Digitales SSL	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)	Metodología para la continuidad de los servicios	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios de Gestión del Cambio en Seguridad de la Información	Metodología para la implementación de los servicios	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios del Centro de Operaciones de Seguridad (SOC)	Procesos de operación implementados: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	Única Vez	15 días naturales posteriores a la emisión del fallo
	Matriz de Escalación Técnica y Organizacional	Única Vez	15 días naturales posteriores a la emisión del fallo
	Procedimiento de operación de la Mesa de Servicios: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	Única Vez	15 días naturales posteriores a la emisión del fallo
	Expedientes Curriculares del personal del SOC	Única Vez	15 días naturales posteriores a la emisión del fallo
Tablero de Estadísticas de Servicios de Seguridad (Portal Único)	Creación de cuentas de acceso en portal único de las soluciones de seguridad	Única Vez	10 días hábiles posteriores al término de la habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo

Entregables bajo demanda
Operbes S.A. de C.V., oferta generar los entregables para los servicios de seguridad, que incluyan, pero no se limiten a, los siguientes conceptos:

Partida 1.

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Borrado Seguro de Información	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado.	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicio de Gestión de Dominios	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos.	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicio de Certificados Digitales SSL	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los certificados que se hayan renovado o adquiridos (incluyendo archivo electrónico compreso con la llave publica relacionado con los requerimientos)	Evento	1 día hábil posteriores a la solicitud generada por parte del Instituto
Servicios de Sistema de Gestión de Seguridad de la Información	Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicios de Gestión del Cambio en Seguridad de la Información	Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicios del Centro de Operaciones de Seguridad (SOC)	Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad	Evento	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto
	Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad	Evento	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme cada solicitud generada por el Instituto
	Actualización de la matriz de escalación	Evento	5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad y Red
	Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad y red	Evento	5 días hábiles posteriores a la ejecución de la ventana mantenimiento

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad y red	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Reporte Técnico de las configuraciones de las soluciones de seguridad y red	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico de los incidentes presentados en las soluciones de seguridad y red	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Reporte Técnico de los requerimientos registrados en la mesa de servicios	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y red, así como su diagrama de interrelación conforme fueron registrados en la CMDB	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Diagramas de Arquitectura de las soluciones de seguridad y red	Evento	2 días hábiles posteriores a la solicitud generada por parte del Instituto

Entregables Periódicos

Operbes S.A. de C.V., oferta generar los entregables para los servicios de seguridad, los cuales incluirán, entre otros aspectos, los siguientes conceptos mínimos:

Partida 1.

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 posteriores 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 posteriores al cumplimiento del mes vencido

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios del Centro de Operaciones de Seguridad (SOC)	Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte de las evaluaciones operativas a los servicios de seguridad implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario
	Reporte que integre el calendario de actualizaciones de versionamiento en *software* de cada servicio implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario

Durante la vigencia del contrato, los entregables requeridos serán presentados en formato electrónico (MS Word, MS Excel, PDF), conforme a los plazos establecidos por el Instituto.

Además, Operbes S.A. de C.V., oferta establecer y mantener un repositorio digital en el que se almacenarán estos entregables como alternativa. Este repositorio estará disponible para consulta durante todo el periodo del contrato. Los permisos de acceso serán definidos por el Instituto durante las reuniones de trabajo, pudiendo ser otorgados al administrador del contrato, al cuerpo de gobierno designado para este propósito, u otros funcionarios designados por el Instituto.

Consideraciones a la finalización del contrato

En caso de terminación anticipada del contrato o al finalizar su vigencia, Operbes S.A. de C.V. será responsable de iniciar el proceso de respaldo de la información, realizar el proceso de baja, llevar a cabo los movimientos de resguardo, traslado y empaquetado de todo el equipo ubicado en las instalaciones del IMSS que forma parte de los servicios y que no constituya parte de las modificaciones, adecuaciones y/o activos que hayan sido realizados como permanentes, o aquellos que de común acuerdo con el IMSS hayan sido sustituidos como parte del servicio.

Una vez concluida la vigencia del servicio, la infraestructura, los componentes habilitadores y los demás elementos utilizados por Operbes S.A. de C.V. para la prestación de los servicios se transferirán al IMSS para garantizar la continuidad operativa. Esta transferencia se realizará mediante un acta de entrega recepción, en la que dichos componentes se transmitirán al IMSS, de manera gratuita y libre de toda limitación de dominio, gravamen y responsabilidad de cualquier naturaleza, conforme a la normativa aplicable al Instituto.

Operbes S.A. de C.V., oferta y acepta que el retiro será coordinado con el tercero que resulte adjudicado, es decir al que se entregue el nuevo contrato o la solución que dará continuidad a la operación del IMSS respecto a los servicios de SERVICIO, observando los acuerdos operativos de migración de un contrato a otro, que contemplen aspectos como la migración de la información de usuario actual hacia la nueva solución.

Operbes S.A. de C.V. oferta y acepta entregar al IMSS, a más tardar 2 meses antes de la finalización del contrato, un plan de trabajo detallado para lograr una transición efectiva de los servicios de seguridad, en el que se incluyan todos los elementos necesarios para llevarlo a cabo. Dicho plan permitirá una transición completa y correcta de los servicios, incluyendo la conformación y actualización de la documentación del proyecto, así como las mesas de trabajo necesarias para dicha transición con los proveedores que den continuidad operativa al proyecto.

La documentación incluirá información generada durante la vigencia del contrato, documentación de los procesos internos de aprovisionamiento, configuración y tareas de operación, soporte y mantenimiento debidamente actualizadas, considerando los eventos de administración de cambios y configuración, incidentes y problemas, además de un inventario actualizado a la fecha de entrega de todos los componentes habilitadores e infraestructura auxiliar que el IMSS solicite para la transición a un nuevo contrato de servicios, con el fin de continuar prestando el mantenimiento preventivo y correctivo a todos los componentes de la solución y diseñar el mecanismo para la renovación tecnológica del resto, minimizando el impacto en la operación.

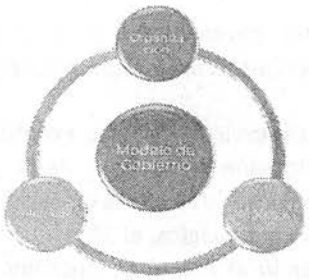
La fecha límite para la entrega de la documentación final actualizada será 2 meses antes de la finalización del contrato SERVICIO. Además, Operbes S.A. de C.V. implementará un esquema de respaldo de la información en cada uno de los componentes que integran los servicios, incluyendo los relacionados con los Centros de Datos del IMSS. El respaldo de la información se almacenará en cada punto táctico para ser entregado al cuerpo de gobierno del contrato para su resguardo, una vez obtenida la autorización correspondiente.

Asimismo, al término del contrato, Operbes S.A. de C.V. 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 previamente presentado por Operbes S.A. de C.V. y aprobado por el IMSS. Durante este período, Operbes S.A. de C.V. proporcionará la orientación tecnológica adecuada al personal del IMSS para garantizar la continuidad de los servicios requeridos, poniendo a disposición del IMSS o de un tercero la transferencia.

Modelo de Gobierno

Operbes S.A. de C.V., oferta y acepta que el Modelo de Gobierno define la estructura operativa y los lineamientos para el proyecto, así como los criterios para evaluar su desempeño. Surgiendo de la necesidad de implementar una estructura orientada a procesos para administrar los "Servicios Administrados de Seguridad Informática SERVICIO", este modelo facilita la colaboración entre todas las partes involucradas para su implementación y operación eficaz.

Este modelo incluye los aspectos clave para asegurar y supervisar la ejecución del proyecto, incluyendo la organización y los roles del Instituto dentro del mismo. Establece esquemas operativos y procesos para que el administrador del contrato, los líderes del proyecto y Operbes S.A. de C.V. (SOC) puedan garantizar los niveles de servicio establecidos en cada etapa de la operación.



La estructura organizacional diseñada para el proyecto de "Servicios Administrados de Seguridad Informática" tiene como objetivo garantizar la eficacia en el trabajo de los responsables, definiendo claramente los roles y responsabilidades en cada nivel.

VII. Cronograma de actividades

ETAPAS	2025											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Transición												
Estabilización												
Implementación												
Mejora Continua												
Termino												

VIII. Niveles de servicio acordados que se cumplirán

El propósito de los Niveles de Servicio es proporcionar al Instituto un método para:

- Evaluar de manera efectiva el rendimiento de los servicios proporcionados por Operbes S.A. de C.V.
- Garantizar que los servicios sean entregados con la calidad esperada.

Los Niveles de Servicio son indicadores definidos por el IMSS que Operbes S.A. de C.V. cumplirá para asegurar la calidad requerida en la prestación del servicio.

En cumplimiento de lo establecido en los artículos 45, fracción XIX, 53 y 53 BIS de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como en los artículos 86 (segundo párrafo), 95, 96 y 97 de su Reglamento, se aplicarán las Penas Convencionales y Deducciones correspondientes por cualquier retraso en las fechas acordadas de entrega o en el inicio de la prestación del servicio, así como por incumplimientos parciales o deficientes en los servicios prestados por Operbes S.A. de C.V.

La aplicación de los niveles de servicio se regirá de acuerdo con lo establecido en los "Términos y Condiciones".

Actualización Tecnológica

Operbes S.A. de C.V., oferta y acepta que El "IMSS" podrá actualizar en cualquier momento las especificaciones de infraestructura, software y hardware mantenidos por SASI, con el fin de proteger a la organización contra la obsolescencia y mantener la tecnología actualizada de los servicios contratados. Por lo tanto, Operbes S.A. de C.V. reconoce y acepta que el "IMSS" está en continua evolución tecnológica. En consecuencia, el "IMSS" notificará a Operbes S.A. de C.V. con diez días hábiles de anticipación, a través del "Administrador del Contrato", para que tome las medidas

necesarias y realice las adecuaciones pertinentes, garantizando así la continuidad operativa del servicio y la actualización de la documentación correspondiente (manuales, diagramas, etc.).

A solicitud del "IMSS", Operbes S.A. de C.V., facilitará servicios de mejora continua y acceso a nuevas características de los servicios proporcionados mediante la actualización tecnológica de la plataforma informática utilizada. Esto permitirá al "IMSS" utilizar los servicios de acuerdo con los Niveles de Servicio establecidos en este Anexo Técnico. Una vez presentada la propuesta de actualización tecnológica, el Modelo de Gobierno evaluará su conveniencia y beneficios para los entornos del "IMSS", decidiendo el momento oportuno y el responsable de llevar a cabo la actualización.

Por lo tanto, Operbes S.A. de C.V., oferta e incluye como alcance de la presente propuesta las actividades relacionadas con la Actualización Tecnológica, que implica la renovación continua de la infraestructura para asegurar que los componentes del sistema se mantengan actualizados conforme a las ofertas del mercado y puedan cumplir satisfactoriamente con los Niveles de Servicio.

Esto incluye, de manera enunciativa:

- Establecimiento, implementación y administración de políticas para actualizar y complementar versiones de software, sistemas operativos, y firmware de equipos.
- Implementación y administración de políticas para actualizar y complementar herramientas de seguridad, monitoreo y gestión con los parches o correcciones necesarias.
- Cumplimiento de las solicitudes de actualización de Componentes Habilitadores requeridas por el "IMSS", incluyendo la sustitución de equipos activos y actualización de software/firmware según las mejores prácticas.
- Análisis proactivo de alertas de software que puedan afectar la infraestructura administrada.
- Certificación del nuevo sistema operativo en un ambiente controlado antes de su instalación en la red de producción, asegurando soporte para nuevas funcionalidades o administración del ciclo de vida del elemento.

Operbes S.A. de C.V., oferta y garantiza que todos los componentes de su solución no se encuentren en situaciones de obsolescencia, como:

- Fin de soporte por parte del fabricante para hardware o software, incluyendo la sustitución o actualización necesaria.
- Falta de acceso a actualizaciones o soporte directo del fabricante, asegurando el acceso continuo a actualizaciones tecnológicas.
- Garantía de cobertura de soporte para equipos y software.

En cumplimiento de este requerimiento, Operbes S.A. de C.V., oferta llevar a cabo las acciones necesarias para la renovación tecnológica de los Componentes Habilitadores del Servicio, incorporando tecnología mejorada que asegure un rendimiento, eficiencia y calidad óptimos.

Adicionalmente, Operbes S.A. de C.V. estará preparado para participar en nuevos proyectos del "IMSS" derivados de la evolución tecnológica, expansión y/o modificación del ambiente operativo, brindando soporte en planificación e implementación según sea necesario.

Propuesta técnica
Servicios Administrados de Seguridad Informática (SASI) 2025

Operbes S.A. de C.V. garantizará el acceso a la información técnica de las tecnologías y productos utilizados en su solución, proporcionando acceso a boletines, publicaciones periódicas y seminarios pertinentes, todo ello incluido en su propuesta sin costos adicionales para el "IMSS".

La implementación de activos de infraestructura, como parte de la actualización tecnológica, será consensuada entre Operbes S.A. de C.V. y el Instituto a través de un plan de trabajo, el cual no podrá exceder 2 meses, una vez que se determine que un servicio sufrirá adecuaciones.

IX. Requerimientos de arquitectura tecnológica

Para atender a los requerimientos de Arquitectura Tecnológica, se remitirá a lo establecido en el presente Anexo Técnico y sus Apéndices A y B.

X. Restricciones e interfaces con otros elementos

Operbes S.A. de C.V. ofeta y aceota que no existen restricciones o interfaces con otros elementos para llevar la implementación y/o continuidad operativa de los servicios establecidos en el presente Anexo Técnico y sus Apéndices A y B.

XI. Pruebas requeridas, método de evaluación y el resultado mínimo que se obtendrá al ejecutar las pruebas.

Operbes S.A. de C.V., oferta y acepta que no se requiere ejecutar pruebas previas para los servicios solicitados conforme el Anexo Técnico y sus Apéndices A y B.

XII. Modificaciones de la especificación técnica de algún bien que no se encuentre regulado por el compendio nacional de insumos para la salud.

No Aplica

XIII. Modificaciones de la especificación técnica de un bien respecto de las estipuladas en el ejercicio anterior.

No Aplica

XIV. Normas: Oficial Mexicana, Estándar (antes mexicana), Internacional, de Referencia o Especificación Técnica, que resulte aplicable a los bienes o servicios requeridos.

Normativa aplicable

Operbes S.A. de C.V. estará sujeto a las políticas internas vigentes del Instituto y a cualquier modificación o inclusión de nuevas políticas que se realicen durante la duración del contrato. Estas políticas aplicables se comunicarán durante las mesas de trabajo; sin embargo, tendrán en cuenta las siguientes, enunciativas, pero no limitativas:

- 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 basadas en el Sistema de Gestión de Seguridad de la Información (SGSI) del Instituto.

- Certificaciones ISO/IEC27001:2022 e ISO/IEC20000-1:2018, vigentes y a nombre del o los licitantes. La presentaciòn de dichas certificaciones es indispensable y su ausencia será motivo de desechamiento de la propuesta, por lo que no pasará la evaluación de puntos y porcentajes.

Cumplimiento de Políticas

Operbes S.A. de C.V. se adherirá estrictamente a las políticas de seguridad en vigor en el Instituto y garantizar en todo momento el cumplimiento de los lineamientos establecidos. En caso de que alguno de estos lineamientos cambie durante la vigencia del contrato, Operbes S.A. de C.V. ajustará su infraestructura y procesos para cumplir con los nuevos requisitos.

Todos los dispositivos informáticos de propiedad de Operbes S.A. de C.V., utilizados en la prestación de los servicios, estarán equipados con sistemas de detección de intrusos, protección contra virus, así como herramientas para detectar y eliminar programas maliciosos como "backdoors" o "troyanos". Esta medida se aplica tanto a dispositivos móviles (laptops, smartphones, tablets, etc.) como a equipos de escritorio (desktop, deskside, etc.) utilizados por el personal asignado para tareas de administración y gestión.

Si estos dispositivos requieren la instalación de sistemas operativos, aplicaciones, antivirus u otras herramientas necesarias para su correcto funcionamiento, así como la adquisición, instalación, mantenimiento y licenciamiento de estos, todos los costos asociados correrán a cargo de Operbes S.A. de C.V.

Bestel

Operbes, S.A. de C.V.
RFC OPE070326DNA

Ciudad de México, a 16 de abril de 2025.

ING. JAVIER CORTÉS LÓPEZ,
Coordinador de Telecomunicaciones y Seguridad de la Información,
Dirección de Innovación y Desarrollo Tecnológico,
Instituto Mexicano del Seguro Social (IMSS).
P r e s e n t e.

Por este medio me permito comunicar a usted que referente a la cotización que presenta mi representada para la integración del procedimiento de investigación de mercado identificado con el **folio No. 047/25**, realizado por la División de Investigación de Mercados de Adquisiciones y Arrendamientos de ese Instituto, para la contratación de los **"Servicios Administrados de Seguridad Informática (SASI)"** del Instituto Mexicano del Seguro Social para el ejercicio 2025, Operbes, S.A. de C.V. mantendrá vigentes todos los certificados señalados en dicha cotización durante la vigencia de la contratación.

Sin otro particular, reciba un cordial saludo.

A T E N T A M E N T E

Luis Alberto De la Garza Aguirre
[redacted] **Representante Legal**
OPERBES, S.A. de C.V.

ANEXOS
DIVISIÓN DE CONTRATOS

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: CARGO Y CORREO ELECTRÓNICO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

ÚLTIMA PÁGINA DE LA PROPUESTA TÉCNICA

Ciudad de México, a 16 de abril de 2025.

ING. JAVIER CORTÉS LÓPEZ,

Coordinador de Telecomunicaciones y Seguridad de la Información,

Dirección de Innovación y Desarrollo Tecnológico,

Instituto Mexicano del Seguro Social (IMSS).

P r e s e n t e.

Última página de la Propuesta Técnica presentada por la empresa Operbes, S.A. de C.V.

ATENTAMENTE

Luis Alberto de la Garza Aguirre

[redacted] Representante Legal

OPERBES, S.A. DE C.V.

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: CARGO Y CORREO ELECTRÓNICO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

Apéndice "A"

Coordinación de Telecomunicaciones y Seguridad de la Información

Servicios Administrados de Seguridad Informática (SASI) 2025

ANEXOS
DIVISIÓN DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

1. Objetivo del Documento

Operbes S.A. de C.V. elabora a continuación el presente documento el cual contiene las especificaciones técnicas y de calidad propuestas.

2. Servicio de Firewall

Especificaciones Técnicas:

- Cumple con el desempeño y capacidades considerando al menos las siguientes especificaciones:

	Tipo 1	Tipo 2	Tipo 3	Tipo 4
Desempeño	5 Gbps	10 Gbps	20 Gbps	240 Gbps
Conexiones simultaneas por seg.	1,000,000	2,000,000	4,000,000	32,000,000
Conexiones nuevas por seg.	50,000	125,000	200,000	1,000,000
Paquetes por seg.	1,000,000	3,000,000	5,000,000	30,000,000
Interfaces 10GbE	8	8	12	12

- Operbes S.A. de C.V. considerará en su propuesta económica que las características de conexiones simultaneas por segundo se refiere a conexiones concurrentes por segundo.
- Incluye un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
- Certificado por organismos de la industria como Common Criteria o ICSA Labs.
- Incluye la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permitir implementar reglas aplicadas a intervalos de tiempo específicos.
- Integrar listas de control de acceso basadas en dirección origen, dirección destino, protocolos, interfaces de red, puertos, URL destino, identidad, rangos de tiempo o periodo.
- Capacidad de agrupar objetos tales como direcciones IP, protocolos y puertos para la simplificación de configuración de políticas de seguridad.
- Capacidad de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con tiempo de espera agotado (timeout).
- Capacidad de implementar mecanismos de calidad de servicio tales como la asignación de ancho de banda a cada tipo de flujo, encolamiento prioritario y moldeado de tráfico (traffic shaping).
- Capacidad de inspeccionar tráfico FTP, HTTP, HTTPS, DNS, ICMP, RADIUS, SMTP y SNMP, H.323, SIP, RSTP, SNMP, entre otros.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Capacidad de segmentar lógicamente el o los activos de infraestructura en dispositivos virtuales (firewalls virtuales); en el que cada instancia virtual es un dispositivo independiente con sus propias políticas de seguridad, interfaces y usuarios administrativos.
- Capacidad de crear hasta 100 instancias de dispositivos virtuales (firewalls virtuales) que serán soportadas en cada uno de los diferentes tipos de firewalls.
- Soportará Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
- Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
- Soportar y operar bajo protocolos de ruteo BGP y OSPF.
- Soportar y operar mediante rutas estáticas.
- Realizar inspección en capa 3 y 4.
- Soporte y operación con al menos 1,000 VLANs
- Integrar esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Contar y operar al menos con una interface Gigabit Ethernet dedicada para administración.
- Generación de bitácoras de eventos (logs) con múltiples niveles de criticidad.
- Incluye una consola centralizada de gestión con las siguientes características:
    - Configuración, de manera centralizada, de políticas en todos los firewalls de la infraestructura.
    - Identificación de qué reglas corresponden a fuentes, destinos y tipos de tráfico.
    - Ejecución de operaciones para grupos o bloques de dispositivos de frontera de seguridad.
    - Capacidad de ofrecer diferentes vistas durante el monitoreo de dispositivos, topologías o políticas.
    - Agrupación de parámetros de configuración para su posterior implementación.
- Durante una actualización de configuración, será capaz de regresar a la configuración anterior, si es necesario o requerido.
- Auditoria de todas las actividades realizadas por los usuarios con privilegios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que incluirá fecha y hora de cada actividad realizada.

3. Servicio de Prevención de Intrusos (IPS)

Especificaciones Técnicas:

- Cumple con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

	Tipo 1	Tipo 2	Tipo 3	Tipo 4
Desempeño	15 Gbps	20 Gbps	24 Gbps	30 Gbps
Conexiones simultaneas / concurrentes por seg.	15,000,000	25,000,000	30,000,000	50,000,000
Conexiones nuevas por seg.	120,000	160,000	200,000	250,000

ANEXO
DIVISIÓN DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

Interfaces 10GbE	4	8	8	8

- Incluye un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Latencia máxima de 0.5 milisegundos.
- Las interfaces de Inspección operarán en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
- Capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado.
- Capacidad de detección en línea sin bloquear tráfico (Modo transparente o supervisión). El sistema sólo alertará que eventos serían bloqueados.
- Capacidad de configuración del modo transparente o supervisión para todo el tráfico o sólo para los paquetes especificados por dirección IP, protocolo, VLAN ID, entre otros.
- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.
- Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
- Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.
- La solución de IPS contemplará que el flujo de información esté asegurado ante una falla en el IPS, pudiendo conmutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.
- Soporte de funcionalidades de alta disponibilidad y configuraciones del tipo activo/activo y activo/failover. Esto será soportado sin degradar el desempeño del IPS y manteniendo las tasas de transmisión requerida.
- Soporte de actualizaciones automáticas de seguridad del archivo de firmas de cuando menos una vez por mes.
- Soporte de análisis de tráfico de voz sobre IP.
- Soporte de monitoreo de VLANs, incluyendo tramas 802.1q
- Soporte de monitoreo de IPv6.
- Soporte de monitoreo con inspección profunda de paquete y monitoreo de paquete en escenarios de alta disponibilidad y con handshake TCP incompleto.
- Reconocimiento de Tuneleo de Protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
- Detección de escaneo de puertos.
- Detección de re-ensamblaje de paquetes fragmentados.
- Captura de tráfico para el análisis de evidencia en formato soportado por TCPDUMP y de manera opcional en formato. ENC (estándar para el software de análisis de protocolos), dicho archivo podrá ser usado para hacer reconstrucción o análisis forense del ataque.
- Integración de Listas Blanca (IP whitelist) mediante una lista de direcciones IP "confiables" que el sistema no bloqueará.
- Integración de firmas definidas por el Instituto mediante el uso de expresiones regulares.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos hosts de la red y crear una alarma cuando cierto umbral sea rebasado.
- Capacidad de integración con el directorio de usuarios (Active Directory y/o LDAP).
- Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
- Administración de seguridad centralizada que incluya las políticas, actualización, respuestas (bloquear, notificar, ignorar, etc.) y opciones de auditoría.
- Consola centralizada que administre los IPS y la integración de usuarios que realice las configuraciones necesarias para remediación de incidentes de seguridad.
- Consola remota con interfaz gráfica o Web cifrada (HTTPS) para el uso en modo de consulta, con diferentes perfiles de usuarios.
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que incluirá fecha y hora de cada actividad realizada.
- Soportará Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
- Capacidad de segmentar lógicamente el o los activos de infraestructura en dispositivos virtuales (IPS virtuales); en el que cada instancia virtual es un dispositivo independiente con sus propias políticas de seguridad, interfaces y usuarios administrativos.
- Operbes S.A. de C.V. considerará en su propuesta económica la capacidad de crear hasta 100 instancias de dispositivos virtuales (IPS virtuales) en todos los equipos ofertados.
- Para los equipos en el centro de datos principal se considera una consola de Administración.

4. Servicios de Protección contra Denegación (DDoS)

	Tipo 1	Tipo 2
Desempeño	20 Gbps	120 Gbps
Conexiones simultaneas por seg.	25,000,000	120,000,000
Conexiones nuevas por seg.	160,000	600,000
Interfaces 10GbE	8	8

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluye un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Operbes S.A. de C.V. considerará en su propuesta que la cantidad de tráfico máximo a inspeccionar por lo equipos y un ancho de banda de los enlaces de internet que estarán recibiendo los equipos, de 1 Gbps para ambos casos.
- Garantizará el paso transaccional de datos legítimos, privilegiando la eliminación de tráfico anómalo dentro de los canales de comunicación del Instituto (Clean Pipes).
- Detección del tráfico basado en el lenguaje TCPDUMP (con información definida en las capas 3 y 4)

DIVISION DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Tendrá la capacidad de advertir anticipadamente algún posible ataque, analizando tendencias de tráfico malicioso en tiempo real.
- Tendrá capacidad de monitoreo en tiempo real de los circuitos dedicados que entregan la conectividad a Internet/Intranet para detectar el comportamiento anormal del tráfico que pueda estar dirigido a atacar las interfaces de los enrutadores implicados en los enlaces.
- Tendrá la capacidad de monitoreo en tiempo real las subredes públicas que conectan los enlaces, para que permita la detección de tráfico anormal que pueda significar un ataque dirigida a ella.
- Detección de ataques basado en la línea de base contra los recursos definidos, con opciones configurables por recursos que permitan filtrar la sensibilidad de la anomalía y disparar un evento de tipo alerta, en paquetes por segundo y bytes por segundo.
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Capacidad de agrupar objetos tales como direcciones IP, protocolos y puertos para la simplificación de configuración de políticas de seguridad.
- Capacidad de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con tiempo de espera agotado (timeout).
- Monitoreará, de manera enunciativa más no limitativa, las siguientes variables en tiempo real:
    - Para el protocolo IP:
        - ICMP
        - Paquetes IP fragmentados
        - Paquetes IP NULL
        - Paquetes IP con direcciones privadas
    - Para el protocolo TCP:
        - Segmentos TCP NULL
        - Segmentos TCP RST
        - Segmentos SYN
        - Tráfico total
- Como mínimo detectará los siguientes tipos de ataques DoS/DDoS sobre las interfaces, subredes y activos de infraestructura:
    - ACK Flood
    - SYN Flood
    - Hogging CPU
    - Chargen (Character generator)
    - FIN Flood
    - ToS Flood
    - DNS Malformed
    - HTTP Flood
    - ICMP Flood
    - UDP Flood
    - Non- UDP/TCP/ICMP Protocol Flood
    - PPS Flood Attack
    - Zombie attack
    - Land Attack

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Permitirá la personalización de los niveles de alarma o umbrales que sirvan para la detección de ataques, a una granularidad por objeto monitoreado.
- Monitoreará actividad sospechosa que pueda significar algún ataque de gusanos, virus, entre otros.
- Monitoreará actividad "Dark IP".
- Detección de anomalías DDoS y amenazas de día cero antes de que impacten en los servicios.
- Detección de zombis (con selecciones de umbrales en bytes por segundos y paquetes por segundos) para clasificar una IP como zombis y con la opción de conocer una lista de zombis activos detectados.
- Protección contra amenazas conocidas
    - Ping de la muerte
    - Ataque por inundación SYN
    - Fragmentacion de paquetes y reensamblaje
    - Broadcast de correo electrónico
    - Saturadores de CPU
    - Scripts generadores de trafico
    - Generadores de caracteres
    - Ataques fuera de banda (WinNuke)
    - Ataque Smurf (generador de gran cantidad de paquetes ICMP)
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que incluirá fecha y hora de cada actividad realizada.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

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

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluye un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Incluirá al menos 4 interfaces 10/100/1000 Gb, expandibles a interfaces 10Gb de ser necesario.
- Tendrá un desempeño de al menos 2Gbps y 1,000,000 conexiones concurrentes
- Capacidad de permitir 50,000 nuevas conexiones por segundo.
- Incluirá la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permitirá implementar reglas aplicadas a intervalos de tiempo específicos.
- Soportará alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Integrará esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Permitirá la creación de grupos de usuarios.
- Permitirá delimitar la cantidad de conexiones por usuarios.
- Permitirá almacenar una base de usuarios local que permita realizar autenticación, sin depender de un servicio de autenticación externo.

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
- Soportará DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKEv2.
- Soportará al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Soportará integridad de datos con md5, sha1 y sha2.
- Soportará las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Establecerá VPNs con gateways con direcciones IP dinámicas públicas.
- Creará una única asociación de seguridad (SA) por par de redes o subredes.
- Realizará VPNs SSL.
- Soportará la conexión desde dispositivos móviles y de escritorio a través de un cliente de acceso remoto. Dicho cliente soportará al menos las siguientes plataformas operativas: MAC OS X desde v10.4.10, iOS desde v4, Android desde v4.2, Windows desde v7.

6. Filtrado de Contenido Web

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluye un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Soportar de forma mínima 120,000 usuarios de forma simultánea.
- Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Permitir operar en modo de proxy explicito y/o proxy transparente.
- Mecanismos de autenticación tales como: archivos locales de contraseña NTLM, LDAP, RADIUS, Active Directory y certificados.
- Control de autenticaciones simultáneas con una misma cuenta de usuario.
- Cifrado de datos (usuario/contraseña) en el proceso de autenticación.
- Controlar e inspeccionar al menos los protocolos: HTTP, HTTPS (SSL), FTP, CIFS, MAPI, DNS, P2P, SOCKS (v4/v5), IM (AOL, MSN, Yahoo Messengers), TCP-Tunnel, MMS, RTSP.
- Catalogar las páginas por dominio (o subdominio), URL o IP.
- Bloqueo de las amenazas emergentes más comunes como: pop-ups, banners, spyware, adware, compartición de archivos punto a punto (P2P file sharing).
- Clasificación en tiempo real de sitios en internet (on-the-fly) que aún no han sido asignados a alguna categoría (servicio automático de validación en línea del sitio para determinar si es malicioso en caso de no tenerlo asignado en alguna categoría).
- Monitoreo y bloqueo de aplicaciones P2P tales como: BitTorrent, eDonkey, Gnutella, Fasttrack.
- Permitir personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
- Permitir la clasificación de URL (dominio o subdominio) o IP en una sola categoría.
- Permitir el uso de expresiones regulares.
- Permitir la creación de categorías de filtrado personalizadas, así como la creación de listas blancas y negras de filtrado URL.
- Capacidad de evitar la ejecución de códigos maliciosos.
- Bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).
- Permitir la recopilación (caching) de páginas web en disco duro y memoria RAM, con el fin de hacer más eficiente el uso de los recursos del equipo.
- Proporcionar capacidades de administración y reporteo centralizado incluyendo control de acceso discrecional, control de versiones, auditoria de usuario, sistema y utilerías de restauración de configuración.
- Proporcionará soporte de administración multisesión (múltiples administradores utilizando el servicio de administración centralizado), a través de una interfaz gráfica vía Web cifrada (HTTPS).
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que incluirá fecha y hora de cada actividad realizada.

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

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluye un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Capacidad de hasta 1.5M de correos por hora
- Con una capacidad de por lo menos 120,000 usuarios
- 12 TB por equipo, en HA por lo menos 24 TB.
- Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Capacidad de revisar tanto el correo entrante como el saliente.
- Escaneará y analizará el asunto, encabezados y el cuerpo de los correos recibidos y enviados.
- Contar con un filtro de contenido para buscar palabras clave en el cuerpo del mensaje, en los encabezados From, To, CC, Subject y en X-Headers. Así mismo, podrá detectar estas palabras en archivos adjuntos.
- Capacidad para poder configurar el tamaño máximo del mensaje y el número de destinatarios del correo tanto a nivel de conexión SMTP, como en políticas cuando el correo ya ha sido recibido.
- Contar con mecanismos para clasificar los remitentes por su origen y tomar decisiones de flujo y volumen en consecuencia. Además, se contará con la facilidad de designar ciertas fuentes de correo en grupos como listas negras, listas blancas o cualquier otro grupo al que deba aplicársele una política específica.
- Capacidad para ofrecer el análisis de archivos comprimidos en los formatos más populares, incluyendo aquellos con 7 capas de compresión.
- Capacidad de detectar el verdadero formato de un archivo y permitir aplicar políticas basadas en este rubro.
- Capacidad para detectar enlaces maliciosos dentro de los correos recibidos en base a la reputación de la URL, utilizando la tecnología de reputación del fabricante, permitiendo la configuración de umbrales para esta detección.
- Contar con un módulo de bloqueo de correo electrónico no deseado con base en la reputación de cuentas de correo, dominios y direcciones IP.
- Capacidad para soportar la revisión de firmas DKIM en los encabezados de correos entrantes.

ANEXOS
DIVISIÓN DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Contar con actualizaciones para sus patrones y motores de detección de spam (heurística), phising y código malicioso.
- Capacidades de colaboración con los centros de investigación de amenazas del fabricante, con la finalidad de reportar de manera automática cualquier comportamiento sospechoso relacionado con el tráfico de correo electrónico.
- Capaz de recibir tráfico con conexiones seguras (TLS) y poder hacer conexiones con otros servidores bajo el mismo protocolo.
- Contar con mecanismos que permitan evitar la recepción de correos de notificaciones dirigidas a cuentas de usuarios no válidos o que no existen en el dominio destino (correos de rebote o Bounced Mails).
- Bloqueo automático de IP debido a alta cantidad de envío de spam, ataque tipo DHA (Directory Harvest Attack), Bounced Mails o código malicioso, totalmente parametrizable al número de mensajes recibidos en un intervalo de tiempo determinado a discreción.
- Capacidad para Integrar excepciones, tanto en hosts remitentes como en destinatarios, así como para cuentas de usuarios o dominios específicos.
- Permitir la creación de cuarentenas o carpetas de auditoría de correo, la cuarentena podrá ser almacenada por la solución como mínimo 30 días.
- Cuando se encuentre contenido malicioso en cuerpo del correo y archivos adjuntos, podrá realizar cualquiera de las siguientes acciones:
    - Reemplazar texto del mensaje afectado.
    - Poner en cuarentena el mensaje completo.
    - Eliminar el mensaje completo.
    - Hacer copia de seguridad (copia del mensaje), para reportarlo con los centros de investigación de amenazas del fabricante.
- Detectar correos masivos con virus y removerlos además de los archivos adjuntos, incluyendo la característica de archivos adjuntos Zero-byte.
- Proporcionar la facilidad de enviar notificaciones a los usuarios (cuentas de correo electrónico) cuando algún evento sospechoso sea detectado.
- Capacidad de integrar agentes que realicen la función de escaneo y detección de spam en activos de infraestructura o servicios de correo electrónico bajo plataformas operativas Linux y/o Windows.
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que incluirá fecha y hora de cada actividad realizada. Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

8. Firewall Especializado en Servicios Web (WAF)

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluye un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Inspección y análisis de perfiles de comportamiento normal de usuarios para detectar y mitigar el uso anormal de aplicativos Web.

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Soportar un throughput de 5 Gbps en capa 7.
- Soportar 100,000 Transacciones por Segundo (TPS).
- Operbes S.A. de C.V. considerará en su propuesta en términos de transacciones por segundo de tráfico HTTPS requiriendo PFS/DH (Perfect Forward Secrecy/ Diffie-Hellman) al menos 60,000 tps
- Servicio de reputación para identificar y bloquear ataques automatizados y/o usuarios maliciosos.
- Detección de ataques por clientes automatizados y robots.
- Detección de URL rewriting u ofuscación del URL.
- Manejo de errores y reescritura de errores para aplicativos Web.
- Capacidad para soportar inspección del protocolo XML.
- Certificado por organismos de la industria como ICSA Labs o PCI.
- Actualización automática de firmas de prevención contra código malicioso.
- Parcheo sobre aplicativos Web contra vulnerabilidades nuevas o conocidas (parcheo virtual).
- Protección contra ataques/vulnerabilidades conocidas (OWASP), de manera enunciativa más no limitativa:
    - SQL injection
    - Cross Site Scripting
    - Cross Site Request Forgery
    - Sensitive Data Exposure
    - Security Misconfiguration
    - Broken Authentication and Session Management
    - Otras nuevas identificadas por OWASP
- Soportar formatos de mensaje:
    - Web 2.0
    - HTML
    - XHML
    - HTML5
    - XML
    - JSON
    - AJAX
    - FLASH
    - JavaScript.
- Soportar Protocolos: TCP v4 y v6, HTTP, HTTPS, SSL/TLS.
- Soportar mitigación de amenazas:
    - HTML Content Aware
    - Intrusion Detection and Prevention (URI patterns)
    - URI rate-based heuristics
    - Vendor Vulnerabilities
    - URL cloaking / rewrite
    - Parameter Inspection
    - Learning mode
- Integridad de transacciones:
    - Session Tracking Cookies, Source/Destination IPs
    - HTTP RFC conformance

ANEXOS
DIVISIÓN DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

  - 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 incluirá fecha y hora de cada actividad realizada.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Soportará Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
- Operbes S.A. de C.V. considerará en su propuesta al menos 200 sitios/portales a proteger.

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

9. Servicios de Gestión Unificada de Amenazas (UTM)

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

	Tipo 1	Tipo 2	Tipo 3	Tipo 4
Desempeño	1 Gbps	2 Gbps	5 Gbps	10 Gbps
Conexiones simultaneas por seg.	10,000	20,000	50,000	100,000
Conexiones nuevas por seg.	150,000	500,000	1,000,000	2,000,000
Interfaces 10/100/1000 Mbps.	4	4	8	8

Operbes S.A. de C.V. considerará en su propuesta que funcionalidad de alta disponibilidad modo Activo/activo y/o Activo/Pasivo.

Operbes S.A. de C.V. considerará en su propuesta que la característica de conexiones simultaneas por segundo" y "conexiones nuevas por segundo, se refiera a conexiones concurrentes por segundo, así como considerar que la suma de las sesiones concurrentes refiere al servicio UTM por cada tipo y las sesiones concurrentes de la tabla de UTM.

Generales

- Incluirá un sistema operativo endurecido propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.

Funcionalidad Firewall

- Estará basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
- Incluirá la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permitirá implementar reglas aplicadas a intervalos de tiempo específicos.
- Soportará y operar bajo protocolos de ruteo BGP y OSPF.
- Soportará y operará mediante rutas estáticas.
- Realizará inspección en capa 3 y 4.

Funcionalidad IPS e IDS

- Soporte de al menos: 1,000,000 conexiones simultáneas por cada Gigabit de inspección.
- Latencia máxima de 0.5 milisegundos.
- Las interfaces de Inspección operarán en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
- El equipo será capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Capacidad de detección en línea sin bloquear tráfico (Modo transparente). El sistema sólo alertará que eventos serían bloqueados.
- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.
- Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
- Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.
- La solución de IPS contemplará que el flujo de información esté asegurado ante una falla en el IPS, pudiendo conmutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.
- Reconocimiento de tuneleo de protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
- Detección de re-ensamblaje de paquetes fragmentados.
- integración de listas blanca (IP whitelist) mediante una lista de direcciones IP "confiables" que el sistema no bloqueará.
- Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos hosts de la red y crear una alarma cuando cierto umbral sea rebasado.

Filtrado de Contenido Web

- Permitirá operar en modo de proxy explicito y/o proxy transparente.
- Controlar e inspeccionar al menos los protocolos: HTTP, HTTPS (SSL).
- Catalogar las páginas por Dominio (o subdominio), URL o IP.
- Permitir personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
- Permitir la creación de categorías de filtrado personalizadas, así como la creación de listas blancas y negras de filtrado URL.
- Capacidad de evitar la ejecución de códigos maliciosos.
- Permitir el bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.
- Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).

Funcionalidad VPN

- Incluirá la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permitirá almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
- Soportará DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKE v2.
- Soportará al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Soportará integridad de datos con md5, sha1 y sha2.

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Soportará las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Establecerá VPNs con gateways con direcciones IP dinámicas públicas.
- Creará una única asociación de seguridad (SA) por par de redes o subredes.
- Soportará Secure Sockets Layer (SSL) versión 3, con al menos los siguientes algoritmos de cifrado simétrico y longitud de llaves: RC4 (128 bits) y 3DES (192bits).

10. Firewall Especializado en Base de Datos (DBF)

Especificaciones Técnicas:

- Tecnología de autoaprendizaje con mínima intervención humana, el proceso será constante y aprenderá estructura de bases de datos, incluyendo schemas, objetos, tablas; sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario.
- Operará a nivel local y en la capa de red
- Soportará al menos los siguientes motores de Bases de Datos:
  - Microsoft SQL Server
  - Oracle
  - Sybase
  - Informix
  - MySQL
  - Progress
  - PostgreSQL
- Proporcionar protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.
- En caso de ser necesario la utilización de agentes, estos soportarán al menos los siguientes Sistemas Operativos:
  - AIX
  - HP-UX
  - Solaris
  - RHEL
  - SusE
  - OEL
  - Windows 32/64 bits
- Capacidad para funcionar independiente a la activación de la auditoría nativa de la base de datos.
- Transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
- Se considera un repositorio para el registro de la actividad, el cual no será accesible por ningún otro mecanismo que no sea la interacción mediante la GUI (interfaz gráfica) proporcionada por el fabricante o por medios administrativos debidamente asegurados.
- Capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de comunicación, y configuración de seguridad, sin importar el sistema operativo sobre el que se encuentren instaladas.

ANEXOS
DIVISIÓN DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Capacidad para poder realizar descubrimientos automatizados en la red para identificar nuevas bases de datos siendo habilitadas, ya sea a nivel de servidor o puertos habilitados en servidores conocidos.
- Capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo a las políticas de negocio. Las definiciones de tipo de dato podrán crearse de manera flexible y granular.
- Capacidad para proveer un servicio de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.
- Apoyará en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y Control de cambios.
- Monitoreará toda la actividad de las bases de datos, y almacenará los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
- Monitoreará e interactuará con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, ligas, stored procedures, entre otros.
- Hará análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.
- Capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.
- Capacidad para proveer detalles sobre alertas ya sean falsos positivos o negativos y tendrá la facilidad de cambiar una política desde la alerta.
- Manejará reglas y políticas tan amplias o granulares como se requieran y podrán ser construidas automática o manualmente y podrán ser actualizadas, igualmente, de forma manual o automática.
- Las políticas granulares para control de acceso o generación de alertas contarán con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios podrán usarse en cualquier número y cualquier combinación:
    - Número de registros a regresar por la consulta (SQL Query)
    - Número de registros afectados
    - Tipo de datos accesado (financiero, recursos humanos, inventarios, o cualquier definición personalizada)
    - Acceso a datos marcados como sensibles
    - Base de Datos, Schema, Instancia, Tabla y Columna 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
- Posibilitará los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.
- Protegerá contra ataques SQL y no-SQL.
- Contar con un mecanismo de actualización de la inteligencia interna de seguridad, que incluye las pruebas de las evaluaciones de vulnerabilidad, las firmas contra ataques, la granularidad de las políticas de seguridad y defensas contra comportamientos conocidos.
- Considerar de emergencia, para potenciales violaciones de la información que incluyan, enunciativa más no limitativamente:
  - Altos volúmenes de acceso a datos sensibles más allá de lo habitual.
  - Acceso a datos inusual para cierta hora del día.
  - Acceso a datos desde una ubicación (física) desconocida.
  - Acceso a datos utilizando aplicaciones/herramientas no autorizadas.
- Manejará una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.
- Tendrá facilidades de Archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP)
- Tendrá la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.
- Contará con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual presentará la documentación respectiva en el descubrimiento de estas.
- Soportará y aplicará simultáneamente un modelo de seguridad positivo y negativo.
- El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que además cumplirá con las siguientes especificaciones:
  - Bloqueará las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
  - Incluirá una lista pre-configurada y detallada de las firmas de ataque.
  - Permitirá la modificación o adición de firmas por el administrador.
  - Permitirá la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
  - Detectará ataques conocidos a nivel base de datos
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Soportará Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).

11. Servicio de Correlación de Eventos

Especificaciones Técnicas:

ANEXOS
DIVISIÓN DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Capacidad para recolectar datos de toda aplicación o dispositivo que tenga una fuente de eventos necesaria para la organización, siendo esto a través de desarrollos predefinidos del fabricante, o con desarrollos personalizados ejecutados por Operbes S.A. de C.V.
- Capacidad para almacenar la información tal y como fue recibida del dispositivo o aplicaciones (eventos en crudo), para efectos de auditoría y análisis forense. La solución generará una firma o "checksum" de los eventos recibidos para garantizar la integridad y mantener la cadena de custodia.
- Permitir la detección automática de fuentes de eventos recolectados a través del protocolo syslog, el cual puede ser enviado vía UDP, TCP o SSL/TLS.
- Capacidad de permitir filtrar eventos por cualquier campo del registro, que son los atributos donde se almacena la información recolectada por la herramienta de las fuentes de eventos.
- Contar con lógica de taxonomía a nivel de la recolección de los eventos, y que permita definir y modificar la misma con base en los eventos auditados.
- Capacidad para detectar automáticamente la desconexión de un conector de integración a través del envío de señales de comunicación para el aseguramiento de la continuidad operativa ("Keep Alive").
- Capacidad para integrarse con los sistemas de detección y prevención de intrusos y los de administración de vulnerabilidades (VM)
- Contar con la capacidad de emitir notificaciones a partir de eventos y datos recopilados a través de mecanismos como SMTP, SNMP y SYSLOG.
- Correlacionar eventos en tiempo real, es decir, que la información de los eventos sobre los que se está basando vendrá del flujo del bus de mensajes.
- Capacidad para definir reglas de correlación con distintos niveles de complejidad, partiendo de las basadas en patrones, hasta reglas basadas en periodos de tiempo, anidadas, causa/efecto y secuenciales.
- El módulo de creación de reglas de correlación tendrá la capacidad de seleccionar eventos para hacer las reglas, así como el seleccionar campos del mismo para ser incluidos en la regla a través de mecanismos como "Drag-and-Drop".
- Contar con la capacidad de probar las reglas antes de ser implementadas en el motor de correlación.
- Comprimirá los datos almacenados al menos con una relación de 10 a 1.
- Contar con mecanismos de monitoreo de la integridad de la información local y archivada.
- Capacidad para soportar de forma nativa la integración con soluciones de almacenamiento en red como SAN, NAS, NFS o CIFS.
- Contar con una suscripción de boletines de seguridad más importantes del mercado para así identificar las vulnerabilidades conocidas, correlacionando la información de herramientas de administración de vulnerabilidades con los eventos recolectados, lo que permitirá automatizar su detección.
- Se considerarán 10,000 eventos por segundo
- Las bitácoras de eventos serán almacenadas por tres meses.

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

Especificaciones Técnicas:

- Detectar cuando un equipo intenta hacer comunicación con un servidor de comando y control en Internet.

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Detectar cuando una amenaza intenta ingresar en la organización mediante internet.
- Detectar e interactuar cuando un atacante o código maliciosos está realizando actividades de movimientos laterales en la organización.
- Detectar ataques del tipo "zero day" que puedan intentar comprometer activos de la organización.
- Tener las capacidades de detección de anomalías en los puntos de la red designados, dicha detección no se basará en firmas ni heurística.
- Tener la capacidad de actuar no solo por la generación de alertas de los componentes tecnológicos implementados, si no capacidades de caza de amenazas.
- Contar con las capacidades de análisis y perfilamiento de los actores detrás de un ataque sobre el Instituto.
- Apoyará al Instituto en la detección y prevención de ataques avanzados, así como el manejo de los incidentes que deriven de ello.
- Elevar el nivel de visibilidad respecto a detección de amenazas avanzadas persistentes.
- Elevar el nivel de capacidades de actuación ante una amenaza avanzada persistente.
- Permitir contar con la información suficiente para identificar el impacto real de una amenaza.
- Permitir proteger diversos segmentos de la red del Instituto con diferentes niveles de protección de acuerdo con la criticidad de los usuarios de cada segmento.
- Permitir tener arquitectura modular y escalable de protección y viabilidad.
- Contar con un servicio especializado que permita apoyar al Instituto en la actuación y respuesta ante un ataque desarrollado con amenazas avanzadas.
- Acortar los tiempos de detección y actuación ante una amenaza avanzada.
- Integrar las capacidades de identificar una amenaza cuando tiene comunicación al exterior mediante el servicio de internet del Instituto o movimiento laterales en las diversas localidades, estas capacidades de detección tendrán la capacidad de perfilar el comportamiento de los usuarios y sus dispositivos con el propósito de detectar cualquier anomalía que puede representar un impacto o riesgo para la Institución
- Disponer de una capa de inteligencia provista por los fabricantes de los componentes tecnológicos y fortalecida por la capa de inteligencia propia de Operbes S.A. de C.V.; dichas capas incluirán al menos las siguientes características:
  - IP, URL Maliciosos
  - Hashes de archivos maliciosos
  - Tácticas, técnicas y procedimientos de los atacantes de la región en organizaciones similares al Instituto.
- Proporcionar las capacidades de realizar investigaciones en profundidad para detectar intrusiones que han pasado desapercibidas para los controles de seguridad implementados, esta investigación permitirá al menos las siguientes capacidades:
  - Caza de amenazas que han estado activas, pero por su comportamiento no han podido ser detectadas.
  - Interacción con el código malicioso y ataques mediante la implementación de trampas en la red y la emulación de servicios.
  - Engaño de los atacantes mediante la implementación de información que pueda rastrear el origen de un ataque.
  - Análisis dinámico de los artefactos detectados.

ANEXOS
DIVISIÓN DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Análisis de indicadores de compromiso en la red de cómputo del Instituto.

- Generar inteligencia accionable con la cual se puedan alimentar los controles preventivos para evitar que una amenaza conocida pueda volver a presentarse o la detección y contención sea temprana.

13. Antivirus

Especificaciones Técnicas:

La solución propuesta por Operbes S.A. de C.V. contará con las siguientes funcionalidades:

- La solución antivirus protegerá a los siguientes sistemas operativos, en las plataformas Intel y AMD (Windows Server 2012 y posteriores).
- La solución antivirus integrará agentes para la detección de virus, malware, entre otros en las plataformas de correo electrónico institucional (Exchange Server 2010 y superiores)
- Reputación Web
  - La solución de antivirus contará con un sistema basado en la reputación de sitios web que permitan de manera proactiva evitar que los usuarios cuando naveguen descarguen componentes maliciosos e infecten sus estaciones de trabajo.
  - El sistema de reputación de archivos estará integrado o desagregado de la consola de antimalware.
  - Niveles de seguridad para evitar la navegación Web a sitios maliciosos cuando los usuarios se encuentran dentro o fuera de la red corporativa.
  - Permitir reclasificar sitios web.
  - El sistema de protección Web no dependerá de ningún explorador en específico.
  - Permitir editar la lista de URL permitidas a nivel general, grupos o personal.
- Ataques de día Zero
  - Cuando es publicada o descubierta una vulnerabilidad en sistema operativo o en alguna aplicación, el Antimalware será capaz de detener un ataque causado por un malware que aprovecha la vulnerabilidad descubierta.
- Protección Antimalware
  - Detectar, analizar y eliminar programas maliciosos, como virus, spyware, gusanos, troyanos, keyloggers, programas publicitarios, rootkits, phishing, entre otros.
  - Detectar, analizar y eliminar, de forma automática y en tiempo real, los programas maliciosos en:
    - Procesos que se ejecutan en la memoria principal (RAM);
    - Archivos creados, copiar, renombrar, mover o modificados, incluyendo períodos de sesiones en la línea de comandos (DOS o shell) abiertos por el usuario;
    - Archivos comprimidos de forma automática, al menos en los siguientes formatos: ZIP, EXE, ARJ, MIME / UU, CAB de Microsoft, Microsoft Comprimir.
    - Archivos recibidos a través de software de comunicación instantánea (Whatsapp, MSN Messenger, Yahoo Messenger, Google Talk, ICQ, entre otros).
  - Detectar y proteger a la estación de trabajo contra acciones maliciosas que se ejecutan en navegadores Web mediante secuencias de comandos en lenguajes tales como JavaScript, VBScript / ActiveX, etc.
  - La detección heurística de virus desconocidos.
- Control de dispositivos

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Proporcionar o restringir el acceso a dispositivos USB, Floppy, CD´s y Carpetas compartidas.
- La solución Antimalware evitará una infección provocada por la ejecución del archivo Autorun.inf contenido en un dispositivo de USB al momento de ser conectado en la estación de trabajo.
- Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware permitirá al usuario hacer modificaciones, control total, solo lectura y ejecución, solo lectura en el contenido del dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger.

• Protección por comportamiento
  - Para aquellos programas que no están permitidos ser ejecutados en la estación de trabajo, serán agregados a una lista de bloqueo de programas específicos.
  - Evitar o monitorear que un programa con comportamiento sospechoso pueda realizar lo siguiente:
    - Duplicar o inyectar archivos de sistema similares.
    - Modificar el archivo de HOST.
    - Incrustar elementos "plugins" en el navegador de Internet Explorer.
    - Instalar librería del programa malicioso.
    - Instale nuevos servicios.
    - Modifique archivos de sistema.
    - Instale servicios o programas para iniciarse al arrancar la estación de trabajo.
• Reporte de amenazas a los laboratorios
  - Capacidad de reportar eventos de amenazas aún no identificadas, de manera automática a través del comportamiento, a los laboratorios de antimalware para el análisis e identificación de la fuente y generación de una protección proactiva.
  - Capacidad de limitar los recursos utilizados para la notificación a los laboratorios, respetando la confidencialidad de la información.
  - Lanzar una política de seguridad en caso de epidemias.
• Métodos de Actualización, Instalación y desinstalación
  - Instalación de cliente antivirus mediante la URL de la Consola de la solución.
  - Instalación de cliente antivirus mediante línea de comandos o script.
  - Lanzamiento de instalación vía navegación de los grupos de trabajo de Windows.
  - Lanzamiento de instalación vía integración con el dominio de Active Directory.
  - Lanzamiento de instalación vía escaneo de equipos dentro de un segmento de Red.
  - Desinstalación del cliente desde el administrador de programas de Windows o el acceso directo a Uninstall.exe del menú inicio.
  - Desinstalación del cliente de forma remota desde la consola de administración.
  - Configuración de Actualizaciones automáticas, así como la fuente de actualización.
  - Distribución de actualizaciones a los clientes de manera Automática y Manual.
  - Actualización de sistema de firmas para clientes sin conectividad al servidor.
  - Actualización de grupo de usuarios por Agentes de Actualización o repositorios.
• Configuración de escaneos
  - Personalización de opciones de escaneo y Acción para una detección en los modos: Manual, en Tiempo Real y Programado.

ANEXOS
DIVISIÓN DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Privilegios de los usuarios
  - Personalizar los permisos de los clientes para realizar acciones en el software local.
  - Inhabilitación de los servicios y/o componentes del Cliente antivirus por medio de contraseña.
  - Habilitar o deshabilitar opciones para el cliente que frecuentemente entra/sale de la red local.

14. Servicios de Prevención de Perdida de Información

Especificaciones Técnicas:

La solución propuesta por Operbes S.A. de C.V. contará con las siguientes funcionalidades:

- Presente un Log de auditoría de todas las actividades de los usuarios.
- Proporcione Reportes predefinidos y personalizados que puedan ser programados o de una sola vez.
- Proporcione un mecanismo de alertas y notificaciones.
- Que sea capaz de proporcionar administración basada en roles múltiples con las siguientes opciones:
  - Capacidad para definir roles de usuarios tales como Administrador, administrador de la seguridad o administrador de cuentas.
  - Capacidad para agregar y modificar roles personalizados.
  - Capacidad de configurar cuentas de usuario y asignar un rol particular a cada usuario.
- Tecnología de Detección.
  - Capacidad para extraer textos de diferentes tipos de documentos para ejecutar escaneos de contenido.
  - Capacidad de realizar detecciones basadas en palabras (keywords) personalizadas o frases (key phrases) personalizadas, con la habilidad de poner diferentes palabras en una sola regla de detección.
  - Capacidad de detección basada en expresiones regulares.
  - Capacidad de detección basada en atributos de archivos tales como tipo de archivo y tamaño de archivo.
  - Capacidad de utilizar validación de reglas de expresión.
  - Capaz de extraer y ejecutar escaneo de contenido de documentos dentro de archivos comprimidos tales como archivos zip y rar.
  - Capaz de controlar la cantidad de capas de compresión que va a descomprimir en archivos comprimidos.
  - Capaz de soportar texto en diferentes idiomas (al menos español e inglés).
  - Que sea capaz de definir identificadores de datos a través de palabras, expresiones o atributos de archivos.
  - Proporcione identificadores de datos predefinidos.
  - Capaz de duplicar y personalizar identificadores de datos predefinidos y personalizados.
  - Capaz de crear identificadores de datos múltiples.
  - Que sea capaz de combinar palabras, expresiones y atributos de archivos dentro de plantillas para identificar información sensible.
  - Proporcione plantillas predefinidas.
  - Con capacidad para importar y exportar plantillas.
  - Capacidad para crear diversas plantillas personalizadas.
  - Capaz de combinar diversas plantillas dentro de una política.

ANEXOS
DIVISIÓN DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

  - Capacidad de crear diversas políticas.
  - Capacidad de crear políticas desde la consola de administración centralizada.
  - Capaz de soportar diversas acciones para una política simple.
  - Capaz de definir un set diferente de acciones basado en la condición de la máquina si está dentro o fuera de la red.
  - Capaz de soportar las siguientes acciones cuando haya fuga de información sensible:
    - Sólo registro del evento (Log violation only).
    - Bloqueo de la transferencia de datos (Block data transfer).
    - Alertas en el equipo del cliente (Client-side alerts).
    - Alertas en el servidor de DLP (Server-side alerting).
    - Almacenamiento de información para análisis forense (Forensic data-capture)
- Será capaz de ejecutar escaneos de contenido en los siguientes canales de información:
  - Correo electrónico
  - HTTP/HTTPS
  - FTP
  - Dispositivos removibles
  - Copia de información a CD/DVD
  - Mensajería instantánea
  - Comando de impresión
  - P2P
  - Portapapeles
  - Correo web
- Capaz de restringir acceso a los siguientes dispositivos:
  - Unidades extraíbles
  - Unidades ópticas
  - IEEE 1394
  - Impresión de pantalla
  - Bluetooth
  - Tarjetas PCMCIA
  - Carpetas compartidas
- Capaz de especificar excepciones de dispositivos
  - Capaz de definir diversas excepciones.
  - Capaz de utilizar comodines cuando se defina una excepción de dispositivos.
  - La configuración de control de dispositivos se realizará de forma centralizada, desde la consola de administración.
  - Capaz de enviar un mensaje de notificación en la computadora del cliente.
  - Capaz de guardar en el log los eventos de control de dispositivos.

15. Generales para todas las soluciones

- Todas las soluciones cumplirán como mínimo con estas especificaciones y capacidades, lo cual son enunciativas más no limitativas.

ANEXOS
DIVISIÓN DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Las propuestas considerarán todos los componentes necesarios para su correcta operación (Equipo activo de Telecomunicaciones, cableado, módulos, etc.)

Las propuestas Técnicas, serán acompañadas de las hojas de especificaciones, trípticos y demás información que permita verificar el cumplimiento de las mismas. Para dar cumplimiento con lo anterior Favor de referirse al APARTADO FOLLETOS y memoriua USB entregada como parte de la presente propuesta.

- Los proveedores podrán realizar propuestas de mejora de cada una de las soluciones y/o diseño de la red con forme a sus propuestas.
- De las propuestas de solución, podrán proponer arreglos tipo cluster.

16. Especificaciones físicas y estándares de conexión para los insumos que conforman los Servicios Administrados de Seguridad Informática 2025

- Especificación y requerimientos de energía eléctrica

Operbes S.A. de C.V. tomó en consideración que El Instituto proporcionará las facilidades dentro de los centros de datos para la alimentación eléctrica (contactos regulados), para el funcionamiento y operación del equipamiento propuesto por Operbes S.A. de C.V., Operbes S.A. de C.V. considerará en su propuesta técnica la característica, cantidad, ubicación y los tipos de contactos requeridos para el aprovisionamiento inicial.

- Especificación y requerimientos de espacio físico y ambiental

El Instituto proporcionará la información específica respecto al espacio físico asignado para que Operbes S.A. de C.V. instale la infraestructura de redes y seguridad en los centros de datos correspondientes. Para tal efecto Operbes S.A. de C.V. para el caso de equipo adicional, especifica lo siguiente relacionado con la cantidad de espacio físico mínimo indispensable que se requerirá para la instalación de la infraestructura de seguridad:
Dado que la presente propuesta es de continuidad de servicios, no se prevé entregar equipamiento adicional por lo que no será requerido espacio físico adicional a menos que se soliciten equipos adicionales a los existentes.

También se contará con las facilidades para su instalación y se apegará al reglamento y políticas internas para la instalación dentro de cada Centro de Datos. Así también indicará las condiciones ambientales adecuadas para el funcionamiento del equipo a instalar para dar el servicio.

- Especificación y requerimiento para el montaje de hardware

Debido a que el requerimiento del Instituto es un servicio administrado, será responsabilidad de Operbes S.A. de C.V. el montaje de los equipos propuestos, racks, gabinetes, rack de panel de parcheo (Parch panel rack), distribuidores fibra óptica, y todo lo necesario para la correcta operación de la solución propuesta, por lo que, en su propuesta económica considerará todo lo necesario con la finalidad de proveer lo necesario.

- Especificación para racks

Operbes S.A. de C.V. cumplirá con las especificaciones de los racks y gabinetes, incluyendo sus dimensiones físicas, para cada uno de los centros de datos donde el Instituto indique para implementar los Servicios SASI 2025, y en apego a las normas y estándares de la industria y los que se acuerdan o indiquen durante las mesas de trabajo con el Instituto.

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Políticas de cableado estructurado en centro de datos

Operbes S.A. de C.V. cumplirá con los requerimientos para cada uno de los Centros de Datos donde el Instituto indique implementar los Servicios SASI 2025, y en apego a las normas y estándares de la industria y los que se acuerdan o indiquen durante las mesas de trabajo con el Instituto, así mismo Operbes S.A. de C.V. suministrará los elementos para la interconectividad necesarios, por lo que: proporcionará e implementará los distribuidores de fibras, las canaletas, los jumpers, y cualquier otro elemento que sea necesario para la correcta interconexión de los racks o puntos de interconexión bajo los estándares de cableado estructurado.

- Especificación de cableado para racks

Operbes S.A. de C.V. contemplará dentro de su propuesta (tanto para el aprovisionamiento inicial, como durante la operación y vigencia del contrato), todo el cableado, jumpers y patch cords necesarios para lograr la interconexión propuesta de todos y cada uno de los módulos y elementos del sistema.

- Especificaciones y requerimientos técnicos de cableado y conectores

Todos los componentes del sistema de cableado, así como troncales de cobre y/o fibra –excepto los correspondientes a los servidores- necesarios para la interconexión de todos los módulos de hardware solicitados para suministrar el servicio de SASI 2025 en el Centro de Datos se incluirán como parte de la propuesta de Operbes S.A. de C.V. y serán sin costo extra para el IMSS. Asimismo, en el caso de incrementos en los servicios estarán incluidos.

- Especificaciones y requerimientos técnicos de equipo de comunicaciones de red

Todos los componentes de interconexión (comunicaciones o balanceo de cargas) que apoyen la operación y administración que se lleve a cabo entre las soluciones de seguridad y red, que por su naturaleza sean requeridos para la puesta en operación del servicio de SASI 2025 en el Centro de Datos, se incluirán como parte de la propuesta de Operbes S.A. de C.V. y serán sin costo extra para el IMSS. Asimismo, en el caso de incrementos en los servicios estarán incluidos.

- Políticas de seguridad de acceso físico a externos

Operbes S.A. de C.V. cumplirá las políticas de seguridad de acceso físico a externos en los centros de datos donde el instituto determine para la provisión de los Servicios correspondientes SASI 2025.

- Especificación y requerimientos de sistema de canalización.

Operbes S.A. de C.V. salvaguardará la integridad física del cableado para evitar fallas potenciales en la operación. De este modo, para salvaguardar la correcta operación del sistema de cableado de fibra óptica y cableado UTP, Operbes S.A. de C.V. utilizará la infraestructura existente en los Centros de Datos y, en general, cumplirá con las norma y políticas de canalización en los mencionados Centros de Datos.

17. Condiciones para los servicios de mantenimiento

Operbes S.A. de C.V. será responsable de realizar las tareas de mantenimiento preventivo y correctivo para la totalidad de la infraestructura dentro del alcance de los servicios de SASI 2025, a través de las labores que considere necesarias y de acuerdo con la estrategia de entrega y soporte de los servicios correspondientes. Enseguida se detallan las condiciones específicas para este servicio.

ANEXOS
DIVISIÓN DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

18. Condiciones para los servicios de mantenimiento preventivo

Como parte del Servicio de Mantenimiento Operbes S.A. de C.V. realizará al menos un mantenimiento preventivo al año a toda la infraestructura que forme parte del contrato de SASI 2025. Para lo cual integrará como parte del servicio, un Plan de Mantenimiento Preventivo, en el cual tomará en cuenta para la proyección de mantenimientos, las ventanas de mantenimiento necesarias, con el fin de ser programadas e informadas con anticipación al administrador del contrato, con objeto de minimizar el impacto a la operación.

En la correspondiente propuesta técnica Operbes S.A. de C.V., incluye como alcance del servicio un Plan de Mantenimiento Preventivo, el cual incluirá como mínimo:

- La descripción de los procesos asociados.
- Los Recursos Humanos y Materiales involucrados.
- Los alcances técnicos del mantenimiento y los protocolos de prueba.
- Las rutas de escalamiento correspondientes.

Esta información se agrupará por tipo de equipo o infraestructura. Para cada caso, Operbes S.A. de C.V. contemplará el calendario de los servicios de mantenimiento preventivo, el cual será validado y autorizado por administrador del contrato, quien revisará que no afecte períodos críticos de la operación del Instituto.

El calendario final de mantenimientos preventivos, fundamentado en el Plan de Mantenimiento Preventivo que se entregará durante las Mesas de Trabajo, será elaborado por Operbes S.A. de C.V. y autorizado por el Instituto, acotando los inmuebles, fechas y actividades a realizar con el máximo detalle, a efectos de coordinar todas las labores necesarias para su correcta ejecución.

19. Condiciones para los servicios de mantenimiento correctivo

Operbes S.A. de C.V. será responsable de realizar el mantenimiento correctivo para los servicios correspondientes de SASI 2022-2024, para lo cual, a continuación integra los procedimientos para reportar un incidente que requiera mantenimiento correctivo, y un ejemplo de matriz de escalamiento con los niveles y tiempos establecidos entre cada nivel.

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

PLAN DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO PARA LOS SERVICIOS DE SEGURIDAD.

Alcance

Aplica para todos los elementos de configuración bajo la responsabilidad del SOC para su operación o gestión, ya sean elementos de configuración propios del SOC o de sus clientes, excluyendo aquellos elementos de configuración provistos por terceros para la operación del SOC y de los cuales el tercero es responsable de los mantenimientos.

Objetivo.

El objetivo principal del procedimiento es asegurar que se cumplan en tiempo y forma los mantenimientos preventivos y correctivo acordados entre el IMSS y OPERBES, con base en lo establecido en el contrato.

Descripción de los Procesos de Mantenimiento Asociados.

Preventivo

Derivado del monitoreo, gestión y manejo de alarmas ó en caso de detectar la necesidad de algún mantenimiento recomendado por el fabricante que evite incidentes que comprometan la disponibilidad, integridad, confidencialidad y continuidad de los servicios, Operbes, S.A. de C.V. analiza previo a su ejecución a través del proceso de control de cambios.

Ventanas de mantenimiento

Operbes, S.A. de C.V. realizarán las ventanas de mantenimiento necesarias, siendo programadas e informadas previamente y con anticipación al administrador del contrato y a todos los involucrados, con el objeto de minimizar el impacto en la operación

Correctivo

Derivado las salidas del proceso de gestión de incidentes y que estas deriven de la necesidad de algún mantenimiento para mitigar el incidente, se analizan previo a su ejecución a través del proceso de control de cambios.

Determinación del nivel de mantenimiento

Puede ser menor o mayor en función de la afectación de la disponibilidad del servicio, es decir, si el cambio no afecta el servicio será considerado como menor sin embargo si es necesario contar con una ventana de tiempo por indisponibilidad del servicio este debe ser considerado como un cambio mayor. Todo esto siempre bajo las politicas del proceso de control de cambios.

ANEXOS
DIVISIÓN DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

Ajustar capacidades

En función de la solicitud y de la planificación, puede ser necesario ajustar los recursos, los umbrales, los horarios, la dotación de personal, las competencias, la automatización, y deben ser supervisados. En el caso de un cambio para implementar una nueva solución o modificar una existente, esta tarea debe apegarse al proceso de control de cambios.

Mantenimiento preventivo

Proceso

Ajustar capacidades

Se realiza plan de mantenimiento preventivo de Hardware y Software los cuales consisten en: Actualización de versiones de sistema operativo (software) previa autorización del personal técnico, así como todos los updates, upgrades y actualizaciones que sean necesarios.

Tareas

El alcance de los servicios de mantenimiento preventivo se ejecuta con las siguientes tareas:

- ✓ Se llevan a cabo rutinas de diagnóstico del buen funcionamiento de la infraestructura, a fin de garantizar el correcto funcionamiento de todos los equipos.
- ✓ Se realizará la actualización de las firmas y/o reglas en los equipos administrados por el SOC con base a las guias y mejores practicas recomendadas por el Fabricante.
- ✓ Se lleva a cabo el diagnóstico para garantizar el correcto funcionamiento de la infraestructura, asimismo en caso de existir se localizará y corregirá la falla.
- ✓ Se entrega reporte con las acciones ejecutadas a la finalización de cada mantenimiento preventivo.
- ✓ Dentro del mantenimiento preventivo, se realizan de ser necesario respaldos de configuración y sistema operativo de los equipos.
- ✓ Se definen en conjunto con el cliente las ventanas de mantenimiento para la realización de las actividades de mantenimiento preventivo, mediante un plan de trabajo.

Protocolos de Prueba

- De acuerdo con el checklist del mantenimiento preventivo del dispositivo a valorar, realizar las actividades de registro correspondientes en la herramienta Service Desk como requerimiento. Realizar la valoración objetiva de:

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

1. Desempeño y salud del equipo como CPU, memoria, disco duro y procesamiento.

2. Verificar el funcionamiento del dispositivo. Estas actividades deberán ser realizadas con una pulsera electrostática para evitar daño en la circuitería de los equipos

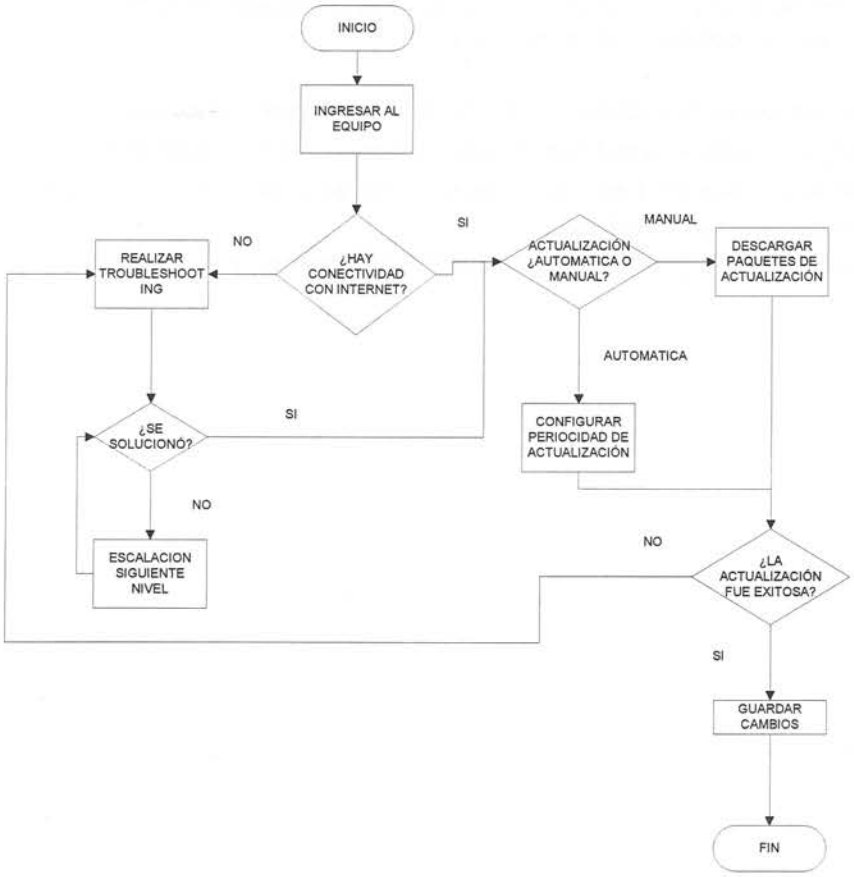
3. Si durante el mantenimiento se detecta una falla, se registra el evento como ticket de soporte en la herramienta de Service Desk y disparar el procedimiento de Soporte a Fallas (Troubleshooting).

4. Realizar el diagnóstico de la falla registrando los resultados del Mantenimiento Preventivo en la orden de trabajo y en la herramienta Service Desk

PROCEDIMIENTO ASOCIADO AL MANTENIMIENTO PREVENTIVO

Se realizará la actualización de las firmas y/o reglas en los equipos administrados por el SOC con base a las guias y mejores practicas recomendadas por el Fabricante

A continuación, se muestra el proceso a seguir:



ANEXOS
DIVISIÓN DE CONTRATOS

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

Recursos humanos involucrados

- Ingeniero de Soporte Técnico

Rol encargado de ejercer la autoridad para garantizar la disponibilidad de la infraestructura previniendo fallas a través de la aplicación de mantenimientos preventivos.
Entre sus principales responsabilidades están:

- Ejecutar el mantenimiento preventivo de acuerdo al calendario y checklist definidos, conservando la integridad, confidencialidad y disponibilidad de los equipos.
- Colaborar en el proceso de soporte a fallas.
- Restaurar y/o corregir las fallas en la infraestructura
- Elaborar ticket de Mantenimiento Preventivo
- Emitir recomendaciones de acuerdo al resultado del mantenimiento preventivo.

- Coordinador de Soporte Técnico

Rol encargado del coordinar y monitorear el servicio de los Ingenieros de Soporte Técnico.
Entre sus principales responsabilidades se encuentran:

- Verificar la ejecución del calendario definido para mantenimientos preventivos.
- Generar solución a los problemas presentados en la operación de los sistemas.
- Coordinar recursos humanos y tecnológicos para el cumplimiento del calendario de mantenimientos preventivos.
- Garantizar el cumplimiento de los mantenimientos preventivos.

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

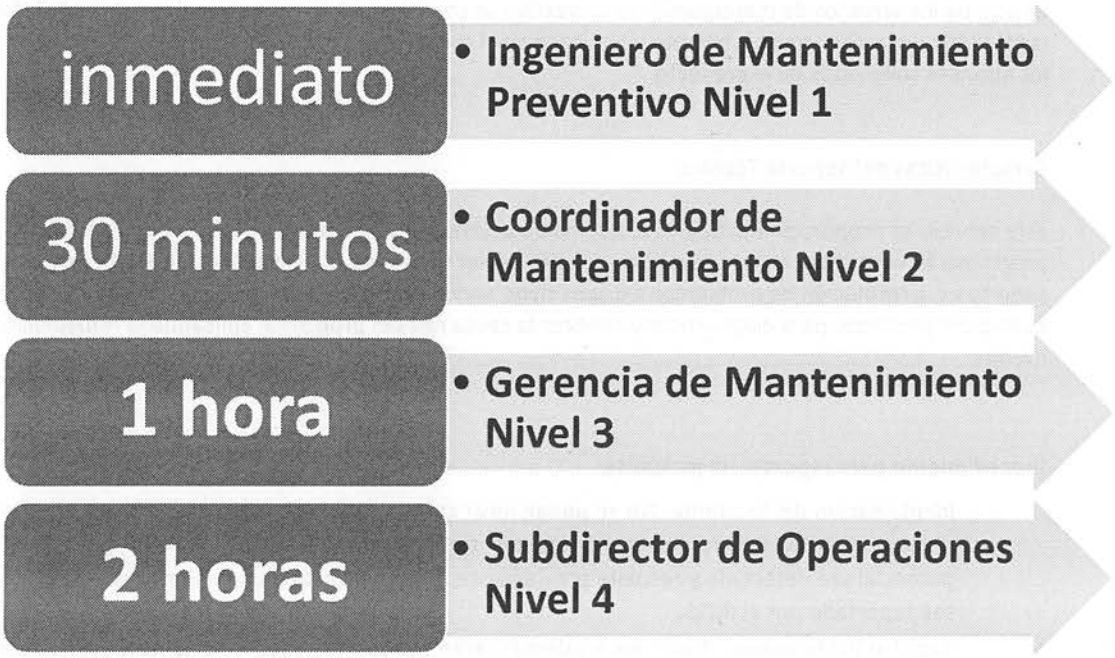
Materiales Involucrados

En cada uno de los eventos de mantenimiento preventivo se tienen considerada la siguiente lista de materiales:

- Herramientas de software
- Dispositivos de almacenamiento para carga de software
- Equipos de prueba.
- Herramientas para limpieza de equipamiento

Niveles de escalamiento

MODELO OPERATIVO DE RUTA DE NIVELES DE ESCALAMIENTO



Mantenimiento correctivo

Se consideran mantenimientos correctivos en caso de falla en infraestructura, bajo la póliza de mantenimiento, contando en caso de aplicar con refacciones necesarias para remplazar las partes dañadas en los tiempos de atención y niveles de servicio pactados.

Este apartado está enfocado a los dispositivos comprendidos en el proyecto los cuales serán sujetos al mantenimiento correctivo correspondiente por parte del personal de Operbes, S.A. de C.V. durante toda la vida del contrato.

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

Soporte Técnico Correctivo: Atención de incidentes, el cual tiene como finalidad estabilizar y garantizar la continuidad del servicio que estos proporcionan al IMSS, ante una falla física de hardware (reparación o reemplazo parcial o total de un dispositivo o servidor) o lógica de dispositivos, servidores y software de redes y seguridad, otorgando soporte técnico de primer, segundo nivel, y tercer nivel directamente con el fabricante de la infraestructura.
El mantenimiento correctivo se llevará a cabo con base en los procedimientos relacionados y tomando en consideración en todo momento los niveles de servicio asignados.

Dentro de los procedimientos de mantenimiento correctivo se tomarán en consideración los siguientes puntos:

- Esquema para reportar el incidente.
- Tiempos establecidos para la escalación entre cada nivel.

Dentro de los servicios de mantenimiento correctivo se contemplará el reemplazo de partes 24x7x4 durante la totalidad de la vigencia del contrato y con base en el cumplimento de los niveles de servicios alineados a los alcances solicitados en el proyecto.

Características del Soporte Técnico

Este servicio es proporcionado bajo el esquema de ocurrencia y de acuerdo a la criticidad del mismo se programarán ventanas de mantenimiento en caso de ser necesario La principal característica de este soporte es la resolución de problemas a dispositivos, servidores y software de la infraestructura considerada dentro del proyecto, para diagnosticar y conocer la causa raíz del problema, aplicando la remediación del mismo.

Procedimiento para reportar un incidente

- Identificación del Incidente: No se puede lidiar con un incidente hasta que éste ocurre. Tan pronto como sea posible todos los componentes serán monitoreados de manera que cualquier falla potencial sea detectada y resuelta previamente, inclusive antes de que el incidente haya afectado y sea reportado por el IMSS.
- Registro del Incidente: Todos los incidentes serán registrados adecuadamente en la herramienta de service desk propuesta y e incluirán al menos, la siguiente información: fecha y hora, nombre de la persona que requiere o a nombre de quien se levanta el incidente, esto si es que se recibe por teléfono, web o correo o inclusive si es un proceso automático detectado por un evento de monitoreo, es decir, contar con un responsable/contacto por parte del IMSS y debidamente identificado.
- Categorizar el Incidente: Parte de los datos en el registro deben contener un código de categoría por el que la llamada o requerimiento fue hecho. Esto es sumamente importante para el proceso de Administración de Problemas, Administración de proveedores y otros procesos de ITSM, ya que nos permite establecer la frecuencia con que una categoría es reportada o los elementos recurrentes relacionados a los mismos.

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

- Priorizar Incidentes: Otro aspecto importante en el registro de cada incidente es acordar un código de priorizar el orden con que los incidentes serán manejados tanto en la herramienta, como con los grupos de soporte.
- Diagnóstico Inicial: La mesa de servicios aplicará un primer diagnóstico generalmente mientras que el usuario se encuentra en el teléfono, a fin de detectar los síntomas del incidente y determinar que puede estar fallando para tomar medidas de solución de primer nivel.
- Investigación y Diagnóstico: En el caso de incidentes donde el usuario solo requiera información, la mesa de servicios la proveerá rápidamente y resolverá el reporte, pero si como resultado del primer diagnóstico se determina que es una falla, se debe tratar como incidente, por lo que se requiere cierto grado de investigación y diagnóstico.
- Recuperación y/o solución: Cuando se ha identificado la solución, ésta debe ser aplicada y comprobada. Todas las acciones deben ser documentadas sin importar que grupo de soporte que resuelve el incidente, en este punto se considera la asistencia a sitio de ser necesario
- Cierre del incidente: La mesa de servicios checara que el incidente fue completamente resuelto y que el usuario está satisfecho y acepta que el incidente sea cerrado.

Proceso de escalamiento

- Prioridad (Alta-Media-Baja)

Cada incidente puede afectar a la organización de forma diferente, es por eso que para poder clasificar el orden en que se deben atenderse normalmente se hace basándose en la prioridad.

La escala para ponderar el impacto acordado de cada elemento de configuración bajo contrato es una escala de tres niveles (Critico [1], Alto [2], Estándar [3], sobre el cual será calificado cada elemento de configuración. El impacto de la solicitud será determinado sobre el nivel de afectación que represente para la operación del cliente la ausencia o fallo del elemento de configuración, así como la relevancia de dicho elemento en su operación. Para ponderar dicho impacto, considere los siguientes criterios:

Crítico. El funcionamiento del elemento de configuración está asociado con el cumplimiento de leyes, regulaciones, normatividades, contratos, acuerdos de nivel de servicio, acuerdos operativos o similares.
Alto. El funcionamiento del elemento de configuración está asociado con el logro de objetivos y metas estratégicas de la organización, incluyendo requerimientos internos sobre la seguridad de la información o la calidad de los servicios provistos.

Estándar. El funcionamiento del elemento de configuración está asociado al desempeño y eficiencia de la organización, sus procesos y procedimientos, incluyendo factores de re-trabajo o merma en la operación.

La escala para establecer la urgencia de la solicitud es con base en el nivel de afectación a la operación asociada a la dilatación en el procesamiento de la solicitud. Para ponderar la urgencia de cada solicitud, se empleará una escala de tres niveles (Alto [1], Medio [2], Bajo (3) sobre la cual será calificada la urgencia para cada solicitud, considerando como guía los siguientes criterios:

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

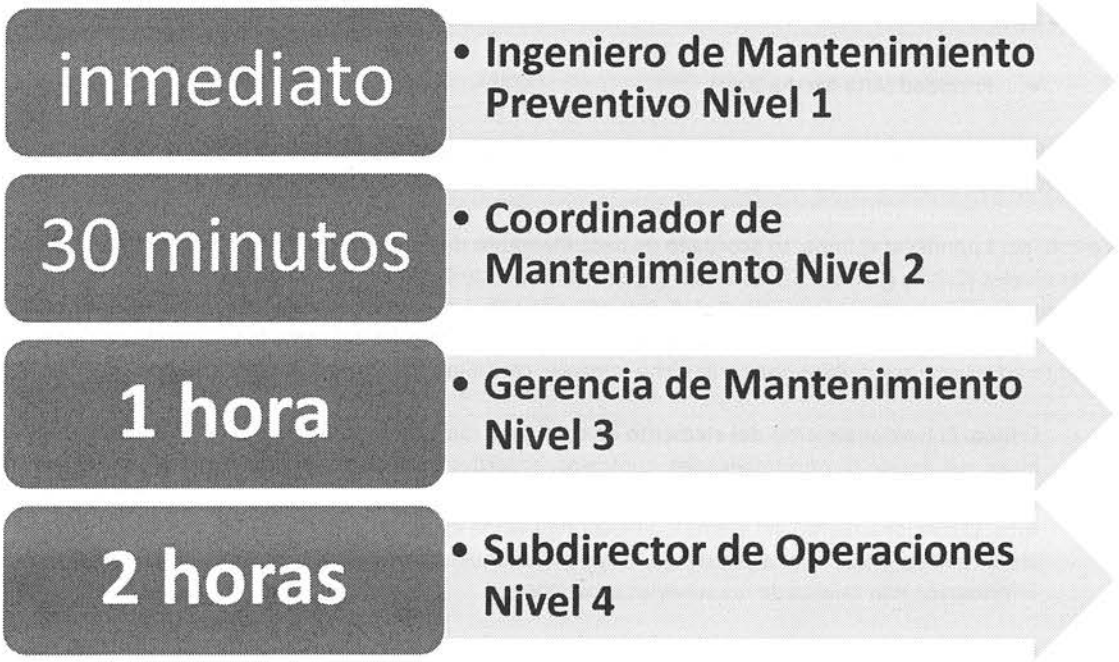
Alta. La operación se ha interrumpido y se requiere aplicar la solicitud para su restablecimiento.

Media. La solicitud es requerida de ser aplicada para mantener los compromisos (tiempo, costo, calidad, cumplimiento, etc.) establecidos para el producto o servicio.

Baja. La solicitud es requerida de ser aplicada como parte de un plan de mejora o para incorporar nuevas funcionalidades no comprometidas para el producto o servicio.

IMPACTO	Urgencia Alta	Urgencia Media	Urgencia Baja
Critico	Prioridad 1	Prioridad 1	Prioridad 2
Alto	Prioridad 1	Prioridad 2	Prioridad 3
Estandar	Prioridad 2	Prioridad 3	Prioridad 3

Niveles de Escalamiento.



Como parte de las Mesas de Trabajo, Operbes S.A. de C.V. proporcionará la Matriz de Escalamiento con los nombres de contactos y responsables.

Apéndice "A"
Servicios Administrados de Seguridad Informática (SASI) 2025

Operbes S.A. de C.V. efectuará el servicio de Mantenimiento Correctivo cuantas veces sea necesario durante la vigencia del servicio, de acuerdo con las especificaciones técnicas del fabricante y consistirá en la reparación o remplazo de las partes dañadas del equipo, cuando ocurra una falla que así lo requiera.

Si el equipo en cuestión no puede ser reparado, se sustituirá por otro equipo de características técnicas iguales o superiores, sin que esto implique la degradación del nivel de servicio requerido para dicho equipo. El tiempo para el reemplazo de partes no excederá los 30 días naturales, durante los cuales Operbes S.A. de C.V. proporcionará un equipo provisional para mantener la operación. El tiempo para el reemplazo de equipos no excederá los 45 días naturales, durante los cuales Operbes S.A. de C.V. proporcionará un equipo provisional para mantener la operación.

SIN TEXTO

Apéndice "B"

Coordinación de Telecomunicaciones

y Seguridad de la Información

Servicios Administrados de Seguridad Informática (SASI) 2025

Apéndice "B"
Servicios Administrados de Seguridad Informática (SASI) 2025

1. Objetivo del Documento

El presente documento que contiene la información considerada por Operbes, S.A. de C.V. para los alcances de continuidad propuestos.

2. Inventario de Activos de Infraestructura – Servicios de Continuidad

CONCEPTO	Sitio	Marca	Modelo	Número Serie
I. Servicios de Seguridad - Continuidad Operativa				
1. Arquitectura de Firewall.				
Tipo 1	IPICYT	Fortinet	FG-1100E	FG10E0TB21900070
Tipo 2	CENATI MONTERREY	Fortinet	FG-1100E	FG10E0TB21900374
	CENATI MONTERREY	Fortinet	FG-1100E	FG10E0TB20903342
Tipo 3	CENATI MÉXICO	Fortinet	FG-1800F	FG180FTK20900846
	CENATI MÉXICO	Fortinet	FG-1800F	FG180FTK20901096
	JALISCO	Fortinet	FG-1800F	FG180FTK20900667
	JALISCO	Fortinet	FG-1800F	FG180FTK20900666
Tipo 4	IPICYT	Fortinet	FG-4200F	FG420FTK20900121
	IPICYT	Fortinet	FG-4200F	FG420FTK20900136
	KIO SANTA FE	Hillstone	SG-6000-X8180	5026640212000634
	KIO SANTA FE	Hillstone	SG-6000-X8180	5018531212004335
	KIO SANTA FE	Hillstone	SG-6000-X8180	5026651212002032
	KIO SANTA FE	Hillstone	SG-6000-X8180	5026640212001736
2. Prevención de Intrusiones (IPS)				
Tipo 1	CENATI MONTERREY	Fortinet	FG-1800F-BDL-950-12	FG6H0ETB21901099
Tipo 2	CENATI MONTERREY	Fortinet	FG-2200E-BDL-950-12	FG2K2ET920900397
Tipo 3	CENATI MÉXICO	Fortinet	FG-3300E-BDL-950-12	FG3K3ET919900293
	CENATI MÉXICO	Fortinet	FG-3300E-BDL-950-12	FG3K3ET919900310
	KIO SANTA FE	Hillstone	SG-6000-E6368P	3016820212002835
	KIO SANTA FE	Hillstone	SG-6000-E6368P	3016820212001026
Tipo 4	IPICYT	Fortinet	FG-3300E-BDL-950-12	FG3K3ET919900331
	IPICYT	Fortinet	FG-3300E-BDL-950-12	FG3K3ET919900323
3. Anti-denegación de servicios DDoS				
Tipo 1	CENATI MONTERREY	Fortinet	FDD-1500F	FI1K5FTE20000010
	CENATI MONTERREY	Fortinet	FDD-1500F	FI1K5FTE20000039

Apéndice "B"
Servicios Administrados de Seguridad Informática (SASI) 2025

Tipo 2	IPICYT	Fortinet	FDD-1500F	FI1K5FTE20000009
	IPICYT	Fortinet	FDD-1500F	FI1K5FTE20000045
	KIO SANTA FE	Netscout	AED8100	CG24227001LA
	KIO SANTA FE	Netscout	AED8100	CG24227027LA
4. Redes Privadas Virtuales (VPN)				
	IPICYT	Fortinet	FG-1100E	FG10E0TB21900305
	IPICYT	Fortinet	FG-1100E	FG10E0TB20903417
	IPICYT	Fortinet	FG-1100E	FG10E0TB20903544
	IPICYT	Fortinet	FG-1100E	FG10E0TB21900273
5. Filtrado de contenido web (WEBFILTERING)				
	IPICYT	Fortinet	FG-1801F-BDL-950-12	FG181FTK20900649
	IPICYT	Fortinet	FG-1801F-BDL-950-12	FG181FTK20900909
	IPICYT	Fortinet	FG-1801F-BDL-950-12	FG181FTK20901026
	IPICYT	Fortinet	FG-1801F-BDL-950-12	FG181FTK20901059
6. Antispam				
	IPICYT	Fortinet	FML-3200E-BDL-641-12	FE3K2ET319000024
	IPICYT	Fortinet	FML-3200E-BDL-641-12	FE3K2ET319000028
	IPICYT	Fortinet	FML-3200E-BDL-641-12	FE3K2ET319000029
	IPICYT	Fortinet	FML-3200E-BDL-641-12	FE3K2ET319000035
7. Firewall Especializado en Servicios Web (WAF)				
	IPICYT	IMPERVA	X10K2	2030BA3322
	IPICYT	IMPERVA	X10K2	2030BA3319
	CENATI MONTERREY	IMPERVA	X10K2	2030BA4461
	CENATI MONTERREY	IMPERVA	X10K2	2030BA4457
	KIO SANTA FE	IMPERVA	X10K2	2227BA1574
	KIO SANTA FE	IMPERVA	X10K2	2227BA1577
8. Firewall de Base de Datos (DBF)				
	IPICYT	IMPERVA	X6520	2030BA3391
	IPICYT	IMPERVA	X6520	2030BA3392
	CENATI MONTERREY	IMPERVA	X6520	2113BA0235
	CENATI MONTERREY	IMPERVA	X6520	2113BA0238
	KIO SANTA FE	IMPERVA	X6520	2221BA2319

Apéndice "B"
Servicios Administrados de Seguridad Informática (SASI) 2025

	KIO SANTA FE	IMPERVA	X6520	2221BA2332
9. Gestión Unificada de Amenazas (UTM)				
Tipo 1	ATLIXCO	Fortinet	FG-100F-BDL-950-12	FG100FTK21003654
	ATLIXCO	Fortinet	FG-100F-BDL-950-12	FG100FTK21003323
Tipo 2	OAXTEPEC	Fortinet	FG-400E-BDL-950-12	FG4H0ETB20902009
	OAXTEPEC	Fortinet	FG-400E-BDL-950-12	FG4H0ETB20902253
Tipo 3	CENATI MONTERREY	Fortinet	FG-1800F-BDL-950-12	FG180FTK21900389
	CENATI MONTERREY	Fortinet	FG-1800F-BDL-950-12	FG180FTK21900326
Tipo 4	CENATI MÉXICO	Fortinet	FG-1800F-BDL-950-12	FG180FTK20901163
	CENATI MÉXICO	Fortinet	FG-1800F-BDL-950-12	FG180FTK20901206
10. Correlación de Eventos				
	IPICYT	Trellix	ETM-5775	A0D2243025
	IPICYT	Trellix	ELM-5775	A0D2238956
	IPICYT	Trellix	ACE-2675	A0D2238969
	IPICYT	Trellix	ERC-1275	A0D2152008
	IPICYT	Trellix	ERC-1275	A0D2201012
	IPICYT	Trellix	DAS-120	A0D3241010
11. Servicio de Protección de Amenazas Persistentes Avanzadas (APT)				
	IPICYT	FireEye	NX6500	3CECEFF33478
	IPICYT	FireEye	NX6500	7CC2552C81E0
12. Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA)				
	IPICYT	CyberArk	THINKSYSTEMSR6504216	J1023ZHY
	IPICYT	CyberArk	THINKSYSTEMSR6504216	J1021R2L
	IPICYT	CyberArk	THINKSYSTEMSR6304210	J1023XX0
13. Servicios de Prevención de Pérdida de Información				
	IPICYT	Trellix	THINKSYSTEMSR6357262	J1020KD5
	IPICYT	Trellix	THINKSYSTEMSR6357262	J1020KD6
14. Servicios De Protección En Redes Inalámbricas y Seguridad en Dispositivos Móviles				
	CENATI MÉXICO	Cisco	MR36	Q3AJ-65ZL-8CNW
	CENATI MÉXICO	Cisco	MR36	Q3AJ-V6SK-VZJP

Apéndice "B"
Servicios Administrados de Seguridad Informática (SASI) 2025

	CENATI MÉXICO	Cisco	MR36	Q3AJ-8JJ6-RN7H
	CENATI MÉXICO	Cisco	MR36	Q3AJ-N8ZE-4CDZ
	CENATI MÉXICO	Cisco	MR36	Q3AJ-5XXG-NA32
	CENATI MÉXICO	Cisco	MR36	Q3AJ-933N-4CJP
	CENATI MÉXICO	Cisco	MR36	Q3AJ-HMEN-EKJA
	CENATI MÉXICO	Cisco	MR36	Q3AJ-P9WS-CP8T
	CENATI MÉXICO	Cisco	MR36	Q3AJ-RJV5-URSR
	CENATI MÉXICO	Cisco	MR36	Q3AJ-RV3H-5NJR
15. Consolas de Gestión				
	IPICYT	FORTINET	FMG-2000E	FMG2KET320000004
	IPICYT	FORTINET	FAZ-3000G	IP VIRTUAL
	IPICYT	FORTINET	FAZ-3000G	FAZ3KGT220000008
	IPICYT	FORTINET	FAZ-3000G	FAZ3KGT220000084
	IPICYT	FORTINET	FAZ-3000G	FAZ3KGT220000033
	IPICYT	FORTINET	FAD-1200F	FAD12FT221000036
	IPICYT	FORTINET	FAD-1200F	FAD12FT221000038
	IPICYT	Imperva	M170	201BA1415
	IPICYT	Imperva	M170	2010BA1467
	KIO SANTA FE	Hillstone	HSA-30D	2106315413647575
	KIO SANTA FE	Hillstone	HSM-500	2106319398019395
	KIO SANTA FE	Lenovo	THINKSYSTEMSR63 04210	J1023XX2
	KIO SANTA FE	Netscout	EDM8000	CG24152038SK
	KIO SANTA FE	Imperva	M170	2227BA2223
	KIO SANTA FE	Imperva	M170	2232BA0370
	CENATI MONTERREY	Imperva	M170	2110BA4189
	CENATI MONTERREY	Imperva	M170	2110BA4176
16. Equipo de Comunicaciones (Switch)				
	IPICYT	CISCO	Nexus 5548UP	SSI15430MJ9
	IPICYT	CISCO	Nexus 5548UP	SSI154600J2
	IPICYT	EXTREME	X670-G2	2122N-41076
	IPICYT	EXTREME	X670-G2	2122N-41091
	KIO	CISCO	2960	FOC1109Z4L9
	KIO	CISCO	2960	FOC1241Y4QV

Operbes, S.A. de C.V. tomo en consideración los activos de infraestructura correspondientes a este apéndice son propiedad del Instituto.

DIVISIÓN DE CONTRATOS

SIN TEXTO

Bestel

Operbes, S.A. de C.V.
RFC OPE070326DNA

Ciudad de México a, 14 de agosto de 2025.

Mtra. Elia Sandra Varas Galeana,
Titular de la Coordinación Técnica
de Adquisición de Bienes de Inversión y Activos
Instituto Mexicano del Seguro Social
P R E S E N T E.

Asunto: Entrega de documentación requerida.

Por medio del presente me dirijo a Usted en calidad de Representante Legal de Operbes S.A. de C.V., para dar continuidad al proceso de la Investigación de Mercado No. 047/25, realizado por la División de Investigación de Mercados de Adquisiciones y Arrendamientos del Instituto Mexicano del Seguro Social para la contratación de los **"Servicios Administrados de Seguridad Informática (SASI)"** para el ejercicio 2025 a la cual fuimos invitados, y para ratificarle que otorgaremos los mismos servicios ofertados en iguales condiciones en cuanto a precio, características y calidad de los bienes y/o servicios de acuerdo a nuestra propuesta presentada el 27 de marzo de 2025 para dicha investigación; dicha propuesta tendrá una vigencia de 30 días hábiles contados a partir del día siguiente a la fecha de recepción del presente.

Asimismo, manifestamos estar inscritos en el registro electrónico de personas físicas y morales en términos de lo dispuesto en el artículo 86 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Agradecemos la confianza depositada en nosotros y reiteramos nuestro compromiso de cumplir con los estándares ofertados, brindándoles un servicio de la más alta calidad, quedando a sus órdenes para cualquier aclaración o información adicional que requiera.

A T E N T A M E N T E

Luis Alberto De la Garza Aguirre
[redacted] y Representante Legal
OPERBES, S.A. DE C.V.

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: CARGO Y CORREO ELECTRÓNICO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

ANEXO 3
DIVISIÓN DE CONTRATOS

Avenida Vasco de Quiroga 2000, Santa Fe, Álvaro Obregón. Ciudad de México. C.P. 01210. Tel: 5540002100

correo electrónico [redacted]

Bestel

Operbes, S.A. de C.V.
RFC OPE070326DNA

Formato de Propuesta Económica
Instituto Mexicano del Seguro Social
Dirección de Innovación y Desarrollo Tecnológico (DIDT)
Coordinación de Telecomunicaciones y Seguridad de la Información

SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMATICA 2025

A	B	C	D	E	F	G
ID	Nombre del servicio	Cantidad Mínima	Cantidad Máxima	Precio unitario de referencia ofertado por el participante	Valor Total Mínimo ofertado por el participante	Valor Total Máximo ofertado por el participante
PARTIDA 1						
1	Licenciamiento Firewall (Tipo 1) - Renovacion	1	1	$ 130,389.96	$ 130,389.96	$ 130,389.96
2	Licenciamiento Firewall (Tipo 2) - Renovación	2	2	$ 145,395.48	$ 290,790.96	$ 290,790.96
3	Licenciamiento Firewall (Tipo 3) - Renovación	4	4	$ 216,149.52	$ 864,598.08	$ 864,598.08
4	Licenciamiento Firewall (Tipo 4) - Renovación	6	6	$ 708,062.73	$ 4,248,376.39	$ 4,248,376.39
5	Licenciamiento IPS (Tipo 1) - Renovación	1	1	$ 692,565.48	$ 692,565.48	$ 692,565.48
6	Licenciamiento IPS (Tipo 2) - Renovación	1	1	$ 1,289,550.96	$ 1,289,550.96	$ 1,289,550.96
7	Licenciamiento IPS (Tipo 3) - Renovación	4	4	$ 745,981.13	$ 2,983,924.50	$ 2,983,924.50
8	Licenciamiento IPS (Tipo 4) - Renovación	2	2	$ 1,391,505.00	$ 2,783,010.00	$ 2,783,010.00
9	Licenciamiento Anti-denegación de servicios DDoS (Tipo 1) - Renovación	2	2	$ 2,064,277.56	$ 4,128,555.12	$ 4,128,555.12
10	Licenciamiento Anti-denegación de servicios DDoS (Tipo 2) - Renovación	4	4	$ 1,106,652.22	$ 4,426,608.87	$ 4,426,608.87
11	Licenciamiento Redes Privadas Virtuales - Renovación	4	4	$ 43,011.96	$ 172,047.84	$ 172,047.84
12	Licenciamiento Filtrado de Contenido Web - Renovación	4	4	$ 738,791.04	$ 2,955,164.16	$ 2,955,164.16
13	Licenciamiento Filtrado de Contenido de Correo (Antispam) - Renovación	4	4	$ 1,117,233.96	$ 4,468,935.84	$ 4,468,935.84
14	Licenciamiento Firewall Especializado en Servicios Web (WAF) - Renovación	6	6	$ 1,807,926.02	$ 10,847,556.10	$ 10,847,556.10
15	Licenciamiento Firewall Especializado en Base de Datos (DBF) - Renovación	6	6	$ 755,507.87	$ 4,533,047.22	$ 4,533,047.22
16	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 1) - Renovación	1	1	$ 16,201.56	$ 16,201.56	$ 16,201.56
17	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 2) - Renovación	1	1	$ 24,241.56	$ 24,241.56	$ 24,241.56
18	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 3) - Renovación	1	1	$ 69,771.00	$ 69,771.00	$ 69,771.00
19	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 4) - Renovación	1	1	$ 135,768.48	$ 135,768.48	$ 135,768.48
20	Licenciamiento Correlación de Eventos - Renovación	2	2	$ 1,469,283.00	$ 2,938,566.00	$ 2,938,566.00
21	Licenciamiento Protección de Amenazas Persistentes Avanzadas (APT) - Renovación	2	2	$ 2,474,064.00	$ 4,948,128.00	$ 4,948,128.00
22	Borrado Seguro de Información	800	2000	$ 650.00	$ 520,000.00	$ 1,300,000.00
23	Gestión de Dominios	1	2	$ 71,591.00	$ 71,591.00	$ 143,182.00
24	Certificados Digitales SSL	8	10	$ 47,489.00	$ 379,912.00	$ 474,890.00
25	Ciberinteligencia	6	12	$ 283,155.83	$ 1,698,934.99	$ 3,397,869.98
26	Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles	800	2000	$ 4,584.91	$ 3,667,925.17	$ 9,169,812.94
27	Gestión de control de acceso para usuarios privilegiados (AAA)	100	200	$ 18,031.00	$ 1,803,100.00	$ 3,606,200.00
28	Antivirus	6000	15000	$ 3,222.52	$ 19,335,108.08	$ 48,337,770.21
29	Prevención de Perdida de Información	1400	3500	$ 6,105.18	$ 8,547,258.70	$ 21,368,146.75
30	Sistema de Gestión de Seguridad de la Información (SGSI)	1	1	$ 298,841.51	$ 298,841.51	$ 298,841.51
31	Servicios de Gestión del Cambio en Seguridad de la Información	1	1	$ 275,853.51	$ 275,853.50	$ 275,853.50
32	Servicios del Cento de Operaciones de Seguridad (SOC)	1	1	$ 7,318,333.96	$ 7,318,333.95	$ 7,318,333.95
33	Consolas de Gestion	17	17	$ 285,315.00	$ 4,850,355.00	$ 4,850,355.00
34	Equipos de Comunicación (Switch)	6	6	$ 19,500.00	$ 117,000.00	$ 117,000.00
PARTIDA 2						
35	Análisis de Vulnerabilidades Estático	60	150	N/A		
36	Análisis de Vulnerabilidades Dinámico	130	325	N/A		
37	Pruebas de Penetración	130	325	N/A		
38	Análisis Forense	2	5	N/A		
				Total sin IVA:	$101,832,011.98	$153,606,053.92

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: CARGO Y CORREO ELECTRÓNICO, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

ATENTAMENTE

Luis Alberto De la Garza Aguirre
[redacted] y Representante Legal
OPERBES, S.A. DE C.V.

Gobierno de México | INSTITUTO MEXICANO DEL SEGURO SOCIAL
SEGURIDAD Y SOLIDARIDAD SOCIAL

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

Oficio No. 09 53 84 61 1CFG/2025/ **7676**

Ciudad de México, a 19 de agosto de 2025.

Asunto: Notificación de Adjudicación.
Adjudicación Directa Nacional: AA-50-GYR-050GYR019-N-157-2025

OPERBES S.A. DE C.V.
P r e s e n t e

El Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información, solicitó la contratación de los "Servicios Administrados de Seguridad Informática (SASI) 2025.

Conforme al documento suscrito por el Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información, mediante el cual dictamina procedente la excepción a la licitación para la contratación de los "Servicios Administrados de Seguridad Informática (SASI) 2025, a través de Adjudicación Directa, con fundamento en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos, 6 fracción IX, 35 fracción III, 53 y 54, fracción II, 57 Y 68 de Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como los artículos 71 y 72 de su Reglamento

En ese sentido, se notifica la aceptación de la confirmación de cotización remitida el **14 de agosto de 2025** y se adjudica la contratación de los **"Servicios Administrados de Seguridad Informática (SASI) 2025" (Partida 1),** conforme a lo siguiente:

Importe Mínimo sin IVA	IVA	Importe Mínimo con IVA	Importe Máximo sin IVA	IVA	Importe Máximo con IVA
$100,700,011.98	$16,112,001.92	$116,812,013.90	$150,776,053.92	$24,124,168.63	$174,900,222.55

Con lo dispuesto en el artículo 67 de la LAASSP, con la presente notificación de la adjudicación del contrato serán exigibles los derechos y obligaciones establecidos en el procedimiento de contratación, sin perjuicio de la obligación de firmar el contrato en la Plataforma Digital de Contrataciones Públicas denominada Compras MX, en la hora y fecha previstas en la propia notificación. La prestación del servicio, así como las condiciones de pago se efectuarán conforme al Anexo Técnico y Términos y Condiciones.

De conformidad con el artículo 37 fracción V de la LAASSP se le informa que la firma del contrato se formalizará en la Plataforma, **dentro de los 15 (quince) días hábiles posteriores a la notificación del presente, en el día y hora que para tal efecto disponga la División de Contratos,** , ubicada en el piso 10 del inmueble de Calle Durango No. 291, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, Ciudad de México; en términos del artículo 57 fracción III de la LAASSP lo anterior. Asimismo, de conformidad con el artículo 69 fracción II de la LAASSP se informa a la empresa adjudicada que deberá entregar la **Garantía de Cumplimiento de Contrato dentro de los 10 (diez) días naturales posteriores** a la firma de este.

En cumplimiento al artículo 84 del Reglamento de la LAASSP y las modificaciones establecidas en el DECRETO por el que se reforman y adicionan diversas disposiciones del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, publicado en el Diario Oficial de la Federación el 1° de junio de 2022, se señalan los datos del contrato derivado del presente procedimiento conforme a lo siguiente:

ANEXOS
DIVISIÓN DE CONTRATOS

Datos de la Garantía de Cumplimiento:

No. De Contrato	050GYR019N**157**25-001-00
Objeto	Servicios Administrados de Seguridad Informática (SASI) 2025 **(Partida 1)**
Monto sin I.V.A. de la garantía	$15,077,605.39
Vigencia del contrato	A partir del día hábil siguiente a la fecha de adjudicación y hasta el 31 de diciembre de 2025.
Tipo de Garantía	Divisible.

Para efectos de la suscripción del contrato respectivo, es necesario que previamente a su firma, a partir del día hábil siguiente a la notificación de la adjudicación, entregue la documentación correspondiente en copia simple y original o copia certificada para cotejo a la **División de Contratos**, en un horario de las 09:30 a las 14:00 horas, 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 (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.
d) Cédula de Registro Federal de Contribuyentes.
e) Comprobante de domicilio con vigencia no mayor a 3 meses.
f) En su caso, escrito de estratificación de empresa en términos del artículo 3 de la Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa.
g) Escrito en términos del artículo 71 y 90, cuarto párrafo de la LAASSP.
h) 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. Los contribuyentes estarán obligados a autorizar al SAT para que se haga público el resultado de la opinión de cumplimiento.
i) Opinión positiva de cumplimiento de obligaciones fiscales en materia de seguridad social, vigente a la firma del contrato, en términos del artículo 32-D del Código Fiscal de la Federación y del Acuerdo 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, el Acuerdo ACDO.AS2.HCT.270422/107.P.DIR, referente a las reglas para la obtención de la citada opinión, publicado el 22 de septiembre de 2022 en el Diario Oficial de la Federación y el Acuerdo ACDO.AS2.HCT.250423/106.P.DIR dictado en sesión ordinaria celebrada el día 25 de abril del 2023, por el que se aprobaron las Disposiciones transitorias aplicables a las Reglas de carácter general para la obtención de la opinión del cumplimiento de obligaciones fiscales en materia de seguridad social, publicadas el 22 de septiembre de 2022 y publicado en el DOF el 04 de mayo de 2023 y el último Acuerdo ACDO.AS2.HCT.270224/34.P.DIR de fecha 27 de febrero de 2024 emitido por el HCT y publicado en el DOF el 21 de marzo de 2024.
j) 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 43 de junio del 2017 y sus modificaciones publicadas en el DOF el 22 de abril de 2024.

- 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.

ANEXO
DIVISIÓN DE CONTRATOS

En cumplimiento a los artículos 5 fracción XI, 66 penúltimo párrafo, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP); 84 segundo párrafo de su Reglamento; así como lo establecido en el Acuerdo por el que se incorpora como un módulo de CompraNet la aplicación denominada Formalización de Instrumentos Jurídicos y se emiten las Disposiciones de carácter general que regulan su funcionamiento, publicado en el Diario Oficial de la Federación; se solicita que previo a la suscripción del contrato respectivo, el Representante Legal del Adjudicado lleve a cabo su registro en el Módulo de Formalización de Instrumentos Jurídicos (MFIJ), para lo cual se pone a su disposición las siguientes direcciones electrónicas: https://comprasmx.buengobierno.gob.mx/mfij#material_de_apoyo

Material de Apoyo Para Proveedores | CompraNet | Gobierno | gob.mx

Se le informa a la empresa adjudicada, que cuenta con un plazo de 30 días naturales, a partir de la formalización del contrato para registrarse y obtener su evaluación en el Registro de Proveedores para la Integridad ante el Instituto Mexicano del Seguro Social REPIIMSS. Para ello deberá ingresar al portal web: https://repiimss.imss.gob.mx/imss/registro

"Manual de Operación del Registro de Proveedores para la Integridad ante el Instituto Mexicano del Seguro Social (REPIIMSS)"
https://www.dof.gob.mx/2024/IMSS/manual_de_operacion_del_registro_de_proveedores_para_la_integridad_ante_el_imss.pdf

Aprobado por el HCT del IMSS en sesión ordinaria de fecha 26 de junio de 2023 mediante Acuerdo ACDO.SA2.HCT.260623/169.P.DA, y publicado en el DOF el 2 de diciembre de 2024 a través del Aviso que puede consultarse en la siguiente liga:

https://www.dof.gob.mx/nota_detalle.php?codigo=5744158&fecha=02/12/2024#gsc.tab=0

Lo anterior, en cumplimiento a la "Política de Integridad para verificar el debido cumplimiento de los proveedores del Instituto Mexicano del Seguro Social", https://www.dof.gob.mx/2024/IMSS/politica_de_integridad_del_imss_2024.pdf

Aprobada por el H. Consejo Técnico (HCT) del Instituto Mexicano del Seguro Social (IMSS) en sesión ordinaria de 30 de mayo de 2023 mediante Acuerdo ACDO.SA2.HCT.300523/137.P.DA, y publicada en el Diario Oficial de la Federación el 2 de diciembre de 2024 a través del Aviso que puede consultarse en la siguiente página:
https://www.dof.gob.mx/nota_detalle.php?codigo=5744157&fecha=02/12/2024#gsc.tab=0

Sin más por el momento, aprovecho la ocasión de enviarle un cordial saludo.

A t e n t a m e n t e

Mtra. Elia Sandra Varas Galeana
Titular de la Coordinación Técnica
de Adquisición de Bienes de Inversión y Activos.
C.c.p.:

Titular de la División de Contratación de Activos y Logística. Presente. (*)
(*) Copia entregada por el Sistema Institucional de Control de Gestión de Correspondencia.

ANEXOS
DIVISIÓN DE CONTRATOS

SIN TEXTO

ANEXOS
DIVISIÓN DE CONTRATOS

Para sello de recepción	SOLICITUD DE ELABORACIÓN DE CONTRATOS	
INSTITUTO MEXICANO DEL SEGURO SOCIAL COORDINACIÓN TÉCNICA DE PLA... CONTRATOS ★ 20 AGO 2025 ★ RECIBIDO DIVISIÓN DE CONTRATOS	**Lugar y Fecha:**	
	Ciudad de México, a 20 de agosto de 2025	
	Oficio:	
	09 53 84 61 1CFG/2025/ 7695	
	Procedimiento:	
	AA-50-GYR-050GYR019-N-157-2025	
	Contratos Totales:	**Alguno Firma DG:**
	(2)	Si: ☐ No: ☒
	Fecha a considerar para cómputo de formalización:	
	☐ Fecha Sello (hasta esta fecha se contó con toda la documentación requerida para formalizar)	☒ Fecha Fallo: (19/Agosto/2025)
Deberá proporcionarse copia del acuse debidamente sellado a la Coordinación de Adquisición de Bienes y Contratación de Servicios		

Lic. Humberto Rincón Juárez
Titular de la División de Contratos
P r e s e n t e.

Me permito solicitar su valiosa intervención a efecto de que tenga a bien girar sus apreciables instrucciones a quien corresponda, para llevar a cabo la elaboración del contrato derivado del procedimiento **de Adjudicación Directa Nacional Electrónica,** cuyo número aparece en el encabezado del presente oficio, para la contratación del **"Servicios Administrados de Seguridad Informática (SASI) 2025)"**, para lo cual en cumplimiento a lo establecido en el Oficio Circular No. 09 53 84 61 1CFA/5094 del 1° de junio del 2021, me permito anexar al presente un Disco Compacto que contiene los documentos electrónicos que se detallan a continuación:

No	Documentación para elaboración de los Contratos	Nombre de los Archivos
1	Oficio de Notificación de Adjudicación	1. Oficio de Notificación de Adjudicación (PDF).
2	Propuestas Económica, Técnica y Legal del licitante adjudicado.	2. PROPUESTA
3	Oficios de designación de la persona servidora pública que fungirá como administrador del Contrato.	3. Administrador del Contrato (PDF).

4

ANEXOS
DIVISIÓN DE CONTRATOS

No	Documentación para elaboración de los Contratos	Nombre de los Archivos
4	Dictamen(es) de Disponibilidad Presupuestal Previos.	4. Dictamen de Disponibilidad Presupuestal Previo (PDF).
5	Anexo Técnico en términos del numeral 4.24.3 y demás numerales aplicables de las Políticas Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social (POBALINES).	5. Anexo Técnico (PDF)
6	Términos y Condiciones en términos del numeral 4.24.4 y demás numerales aplicables de las POBALINES.	6. Términos y Condiciones (PDF).
7	Requisición de Bienes y Servicios (FO-CON-3)	7. FO-CON-3 (PDF).
8	Justificación de la excepción	8. Justificación de la excepción

Es importante precisar que, de conformidad con lo establecido en el **Oficio de Notificación de Adjudicación** ya referido, se indicó al proveedor adjudicado que deberá entregar la documentación correspondiente para la formalización del citado instrumento jurídico en esa División de Contratos.

No omito señalar la importancia de salvaguardar y custodiar la información contenida en el medio magnético adjunto.

Sin más por el momento, aprovecho la ocasión de enviarle un cordial saludo.

A t e n t a m e n t e

Mtra. Elia Sandra Varas Galeana
Titular de la Coordinación Técnica de Adquisición
de Bienes de Inversión y Activos

Con copia para:
División de Contratación de Activos y Logística. Presente. (*)
Sistema Institucional de Control de Gestión de Correspondencia).

ESVG//BHC/MOSS

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** **050GYR019N15725-001-00**

OTIS

ANEXO 4 (CUATRO)

"DOCUMENTO DE DESIGNACIÓN DE ADMINISTRADOR DEL PRESENTE CONTRATO"

ANEXOS
DIVISIÓN DE CONTRATOS

DIVISIÓN DE CONTRATOS
NIVEL CENTRAL

SIN TEXTO

Gobierno de México | INSTITUTO MEXICANO DEL SEGURO SOCIAL
SEGURIDAD Y SOLIDARIDAD SOCIAL

ACUSE

Dirección de Innovación y Desarrollo Tecnológico
Coordinación de Telecomunicaciones y Seguridad de la Información

Of. N° 09 52 17 61 5A00/2025/0304
Ciudad de México, a 13 de agosto de 2025

Ing. Deyanira Ramírez Ramos
Coordinadora de Servicios Administrativos
P r e s e n t e.

Me refiero al procedimiento de contratación para el servicio de los **"Servicios Administrados de Seguridad Informática (SASI) 2025"**, para el ejercicio 2025.

Sobre el particular, 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 el suscrito, C. Ing. Javier Cortés López fungirá como **"Administrador del Contrato"**, con fundamento en lo dispuesto por los artículos 2 fracción V, 74, y 84 del Reglamento Interior del Instituto Mexicano del Seguro Social; numeral 4.17 y 5.3.15 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social, y conforme a lo previsto en el numeral 7.1.8., del Manual de Organización de la Dirección de Innovación y Desarrollo Tecnológico vigente.

Asimismo, me comprometo a desempeñar el cargo 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.

- Datos de la persona servidora púbica que fungirá como administrador del contrato:
  - **Nombre completo:** Ing. Javier Cortés López
  - **Cargo**: Coordinador de Telecomunicaciones y Seguridad de la Información
  - **Área de adscripción en el IMSS**: Dirección de Innovación y Desarrollo Tecnológico
  - **Domicilio institucional**: Avenida Paseo de la Reforma número 476, Anexo de Telecomunicaciones, Colonia Juárez, Ciudad de México, Código Postal 06600. Anexo de Telecomunicaciones, PA.
  - **RFC:** [redacted]
  - **CURP** [redacted]
  - **Correo electrónico**: javier.cortesl@imss.gob.mx
  - **Teléfono institucional: 52 3827 00 ext. 11190**

DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO
COORDINACIÓN DE SERVICIOS ADMINISTRATIVOS
14 AGO. 2025 12:19
OFICIALÍA DE PARTES

Sin otro particular por el momento, le envío un cordial saludo.

Atentamente,

Ing. Javier Cortés López
Coordinador de Telecomunicaciones y Seguridad de la Información

SIN ANEXO

(*) Las copias se envían mediante SICGC
- **Mtra. Claudia Laura Vázquez Espinoza. - Titular de la Dirección de Innovación y Desarrollo Tecnológico**

JCL/AGC

2025 Año de La Mujer Indígena

ANEXOS
DIVISIÓN DE CONTRATOS

SE CANCELAN DATOS PERSONALES DE PERSONA(S) FISICAS IDENTIFICABLE(S) TALES COMO: RFC Y CURP, POR CONSIDERARSE INFORMACIÓN CUYA DIFUSIÓN PUEDE AFECTAR A LA ESFERA PRIVADA DE LA MISMA, DE CONFORMIDAD CON LO ESTABLECIDO EN LOS ARTÍCULOS 115 Y 120 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. D.O.F. 20-marzo-2025

SIN TEXTO