CONTRATO **ABIERTO** PARA LA PRESTACIÓN DEL **SERVICIO ADMINISTRADO DE CIBERSEGURIDAD**, CON CARÁCTER **NACIONAL** QUE CELEBRAN, POR UNA PARTE, EL EJECUTIVO FEDERAL POR CONDUCTO DEL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES, EN LO SUCESIVO **"EL INSTITUTO FONACOT"**, REPRESENTADO POR LA **C. JAZMÍN GARCÍA JUÁREZ**, EN SU CARÁCTER DE **APODERADA LEGAL**, Y POR LA OTRA, **IQSEC, S.A. DE C.V.**, EN LO SUCESIVO **"EL PROVEEDOR"**, REPRESENTADO POR LA **C. YOLANDA SALDAÑA TAVERA**, EN SU CARÁCTER DE **APODERADA LEGAL** A QUIENES DE MANERA CONJUNTA SE LES DENOMINARÁ **"LAS PARTES"**, AL TENOR DE LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

DECLARACIONES

I. **"EL INSTITUTO FONACOT"** declara que:

I.1 Es una **"ENTIDAD"** de la Administración Pública Federal, de conformidad con lo establecido en la Ley del Instituto del Fondo Nacional para el Consumo de los Trabajadores, publicada en el Diario Oficial de la Federación el 24 de abril del 2006, cuya competencia y atribuciones se señalan en el citado ordenamiento legal.

I.2 Conforme a lo dispuesto por la **escritura pública número 194,807 de fecha 27 de noviembre de 2023, otorgada ante la fe del Lic. Amando Mastachi Aguario, notario público número 121 de la Ciudad de México, documento que quedó debidamente inscrito en el Registro Público de Organismos Descentralizados, bajo el folio 82-7-29122023-120340,** la **C. Jazmín García Juárez**, en su cargo de Subdirectora General de Administración, es la servidora pública 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 57, fracción IV del Estatuto Orgánico del Instituto del Fondo Nacional para el Consumo de los Trabajadores de fecha 04 de abril del 2025,** suscribe el presente instrumento el **C. Ricardo Oria Esquivel**, en su calidad de Subdirector General de Tecnologías de la Información y Comunicación, con **R.F.C. OIER8103266T3**, **designado para dar seguimiento y verificar** el cumplimiento de las obligaciones que deriven del objeto del presente contrato, quien podrá ser sustituido en cualquier momento, bastando para tales efectos un comunicado por escrito y firmado por el servidor público facultado para ello, informando a **"EL PROVEEDOR"** para los efectos del presente contrato.

I.4 De conformidad con el **apartado VII, numeral 13 inciso b) de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del Instituto FONACOT,** suscribe el presente instrumento el **C. Fernando Zepeda Delgadillo**, Director de Recursos Materiales y Servicios Generales, **R.F.C. ZEDF7412252J5,** facultado para actuar en calidad de área contratante.

I.5 La adjudicación del presente contrato se realizó mediante el procedimiento de **Adjudicación Directa** de carácter **Nacional**, al amparo de lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; **33, 35 fracción III, 54 fracción III y 68 fracción I** de

la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"LAASSP"**, **71, 72 fracción III y 85** de su Reglamento.

I.6 **"EL INSTITUTO FONACOT"** cuenta con suficiencia presupuestaria otorgada **mediante oficio número DICP/SP/2025/105 de fecha 3 de septiembre de 2025**, emitido por la Dirección de Integración y Control Presupuestal de **"EL INSTITUTO FONACOT"**.

I.7 Cuenta con el Registro Federal de Contribuyentes **N° IFN060425C53**.

I.8 Tiene establecido su domicilio en Avenida Insurgentes Sur número 452, Colonia Roma Sur, Demarcación Territorial Cuauhtémoc, Código Postal 06760, Ciudad de México, mismo que señala para los fines y efectos legales del presente contrato.

II. **"EL PROVEEDOR"**, por conducto de su Representante Legal declara que:

II.1 Es una persona **moral** legalmente constituida mediante la **escritura pública número 79,927 de fecha 23 de agosto de 2007, otorgada ante la fe del Lic. Jorge Alfredo Domínguez Martínez, titular de la notaría pública número 140 y el Lic. Alejandro Domínguez García Villalobos, titular de la notaria 236 como asociado del entonces Distrito Federal, ahora Ciudad de México**, denominada **IQSEC, S.A. DE C.V.,** cuyo objeto social es entre otros **comprar, vender, distribuir, subdistribuir, importar, arrendar, exportar y comercializar en general, toda clase de productos, mercancías, artículos y cualquier bien que este en el comercio y en consecuencia sea susceptible de apropiación particular, enunciativa y no limitativamente toda clase de computadoras, sistemas de seguridad informática, sistemas de seguridad física, circuitos cerrados de televisión, enlaces de telecomunicaciones, equipos electrónicos de comunicación móvil para localización, programas y sistemas de cómputo, de información geográfica, para localización de unidades móviles, objetos y personas, mapas digitales y cartografía, equipos, componentes, mobiliario y accesorios relacionados con la actividad computacional, de telecomunicaciones y de oficina, elementos tecnológicos relacionados y "hardware y software" en general**, inscrita en el Registro Público de Comercio, bajo el folio mercantil número 371652 de fecha 23 de octubre de 2007.

II.2 La **C. Yolanda Saldaña Tavera**, en su carácter de apoderada legal, cuenta con facultades suficientes para suscribir el presente contrato y obligar a su representada, como lo acredita con **la escritura pública número 96,546 de fecha 18 de febrero de 2014, otorgada ante la fe del Lic. Jorge Alfredo Domínguez Martínez, titular de la notaría pública número 140 del entonces Distrito Federal hoy Ciudad de México,** mismo que bajo protesta de decir verdad manifiesta no le ha sido limitado ni revocado 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 **IQS0708233C9.**

II.5 Acredita el cumplimiento de sus obligaciones fiscales en términos de lo dispuesto en el artículo 32-D del Código Fiscal de la Federación vigente, incluyendo las de Aportaciones Patronales y

Entero de Descuentos, ante el Instituto del Fondo Nacional de la Vivienda para los Trabajadores y las de Seguridad Social ante el Instituto Mexicano del Seguro Social, conforme a las Opiniones de Cumplimiento de Obligaciones Fiscales emitidas por el SAT, INFONAVIT e IMSS, respectivamente.

II.6 Tiene establecido su domicilio en Avenida Patriotismo 399, Colonia San Pedro de los Pinos, Demarcación Territorial Benito Juárez, Ciudad de México, México, C.P. 03800, mismo que señala para los fines y efectos legales del presente contrato.

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 FONACOT"** la prestación del **SERVICIO ADMINISTRADO DE CIBERSEGURIDAD**, en los términos y condiciones establecidos en este contrato y sus **Anexos I. y II. Anexo Técnico y Cotización** respectivamente, que forman parte integrante del mismo.

SEGUNDA. MONTO DEL CONTRATO.

"EL INSTITUTO FONACOT" pagará a **"EL PROVEEDOR"** como contraprestación por los servicios objeto de este contrato, la cantidad mínima de **$10,053,160.00 (Diez millones cincuenta y tres mil ciento sesenta pesos 00/100 M.N.)** más impuestos por $1,608,505.60 (Un millón seiscientos ocho mil quinientos cinco pesos 60/100 M.N.) y un monto máximo de **$25,132,902.00 (Veinticinco millones ciento treinta y dos mil novecientos dos pesos 00/100 M.N.),** más impuestos que asciende a $4,021,264.32 (Cuatro millones veintiún mil doscientos sesenta y cuatro pesos 32/100 M.N.)

El precio unitario es considerado fijo y en moneda nacional **(pesos)** hasta que concluya la relación contractual que se formaliza, incluyendo todos los conceptos y costos involucrados en la prestación del **SERVICIO ADMINISTRADO DE CIBERSEGURIDAD,** 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 FONACOT"** no otorgará anticipo a **"EL PROVEEDOR".**

CUARTA. FORMA Y LUGAR DE PAGO.

"EL INSTITUTO FONACOT" efectuará el pago a través de transferencia electrónica en pesos de los Estados Unidos Mexicanos, a mes vencido conforme a los servicios efectivamente prestados y a

entera satisfacción del administrador del contrato y de acuerdo con lo establecido en el **"Anexo I"** que forma parte integrante de este contrato.

"EL INSTITUTO FONACOT" realizará el pago en un plazo máximo de 17 (diecisiete) días hábiles siguientes, contados a partir del envío y verificación del Comprobante Fiscal Digital por Internet (CFDI) o factura electrónica a través de la Plataforma, y con la aceptación del Administrador del presente contrato, previa entrega de los servicios.

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 deberá ser presentada con el visto bueno del administrador del contrato y con los requisitos fiscales vigentes señalados en los artículos 29 y 29-A del Código Fiscal de la Federación aplicable en los Estados Unidos Mexicanos, por lo que deberán:

A. Presentar comprobantes fiscales digitales por Internet (CFDI), en archivo XML y la representación de dichos comprobantes en documento impreso en papel, que reúnan los requisitos fiscales respectivos, en la que indique el servicio prestado y el número de contrato que lo ampara. Dichos comprobantes serán enviados y entregados de conformidad con lo solicitado en el **Anexo I**, mismos que deberán de ser entregados en las oficinas centrales del Instituto FONACOT, ubicadas en Av. Insurgentes Sur No. 452, Col. Roma Sur, C.P. 06760, Demarcación Territorial Cuauhtémoc, Ciudad de México, en la Subdirección General de Tecnologías de la Información y Comunicación, así mismo deberá ser enviada a los correos electrónicos: gerardo.daza@fonacot.gob.mx y ricardo.oria@fonacot.gob.mx en un horario de labores de las 9:00 a las 18:00 horas de lunes a viernes en días hábiles.

B. Los comprobantes fiscales deben emitirse por los actos o actividades que se realicen, dichos comprobantes deben de cumplir con las especificaciones que determine el Servicio de Administración Tributaria (SAT), considerando el Anexo 20 "Guía de llenado de los comprobantes fiscales digitales por Internet".

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 FONACOT",** para efectos del pago.

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

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 FONACOT"** en el **Anexo I** del presente contrato.

Los servicios serán prestados en los domicilios señalados en el **Anexo I** y fechas establecidas en el mismo;

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 I para la reposición o corrección, contados a partir del momento de la notificación por correo electrónico y/o escrito, sin costo adicional para **"EL INSTITUTO FONACOT"**.

SEXTA. VIGENCIA.

"LAS PARTES" convienen en que la vigencia del presente contrato será del **1 de noviembre** al **31 de diciembre de 2025.**

SÉPTIMA. MODIFICACIONES DEL CONTRATO.

"LAS PARTES" están de acuerdo que **"EL INSTITUTO FONACOT"** 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 contrato esté vigente. La modificación se formalizará mediante la celebración de un Convenio Modificatorio.

“EL INSTITUTO FONACOT”, 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 FONACOT”**, 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 FONACOT”** 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 FONACOT” 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 un 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

A) CUMPLIMIENTO DEL CONTRATO.

Conforme a los artículos 69, fracción II, 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 del **“INSTITUTO FONACOT”,** por un importe equivalente al **10%** del monto máximo del contrato, sin incluir el IVA.

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

Si las disposiciones jurídicas aplicables lo permiten, la entrega de la garantía de cumplimiento se podrá realizar de manera electrónica.

En caso de que **"EL PROVEEDOR"** incumpla con la entrega de la garantía en el plazo establecido, **"EL INSTITUTO FONACOT"** podrá rescindir el contrato y dará vista al Órgano Interno de Control 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 FONACOT"** 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 FONACOT",** dentro de los 10 (diez días) naturales siguientes 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 FONACOT"** 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 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 FONACOT"** 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, de conformidad con el artículo 107 del Reglamento de la **"LAASSP"**.
- **e)** Mantener al corriente sus obligaciones fiscales durante la vigencia del presente contrato.

DÉCIMA PRIMERA. OBLIGACIONES DE "EL INSTITUTO FONACOT".

"EL INSTITUTO FONACOT", 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 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.

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

"EL INSTITUTO FONACOT" designa como Administrador del presente contrato al **C. Ricardo Oria Esquivel**, en su calidad de Subdirector General de Tecnologías de la Información y Comunicación, con **R.F.C. OIER8103266T3** quien dará seguimiento y verificará el cumplimiento de los derechos y obligaciones establecidos en este instrumento.

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

"EL INSTITUTO FONACOT", a través del administrador del 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 FONACOT" 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 calcularan conforme a lo establecido en el **Anexo I**. 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 para lo cual deberá emitir un Comprobante Fiscal Digital por Internet tipo egreso y contará con un plazo que no excederá de 5 (cinco) días hábiles contados a partir de la fecha de la notificación **correspondiente**, en favor de "**EL INSTITUTO FONACOT**". En caso de negativa se procederá a hacer efectiva la garantía de cumplimiento del contrato.

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

El cálculo de las deducciones correspondientes las realizará el administrador del contrato de **"EL INSTITUTO FONACOT",** cuyá notificación se realizará por escrito o vía correo electrónico, dentro de los **5 días hábiles** posteriores al incumplimiento parcial o deficiente.

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 I**. "**EL INSTITUTO FONACOT**" por conducto del administrador del contrato aplicará la pena convencional.

El Administrador determinará el cálculo de la pena convencional, cuya notificación se realizará por escrito o vía correo electrónico, dentro de los **5 días hábiles** posteriores al atraso en el cumplimiento de la obligación de que se trate.

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 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 contrato.

El pago de la pena podrá efectuarse a través de un Comprobante Fiscal Digital por Internet tipo Egreso, conocido comúnmente como nota de crédito, relacionado con el folio fiscal del CFDI próximo a pagar y contará con un plazo que no excederá de **5 (cinco) días hábiles** contados a partir de la fecha de la notificación correspondiente, a favor de "**EL INSTITUTO FONACOT**".

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

DÉCIMA QUINTA. LICENCIAS, AUTORIZACIONES Y PERMISOS.

"EL PROVEEDOR" se obliga a observar y mantener vigentes las licencias, autorizaciones, permisos o registros requeridos para el cumplimiento de sus obligaciones.

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 trasportar los bienes e insumos necesarios para la prestación del servicio, desde su lugar de origen, hasta las instalaciones señaladas en el **ANEXO I** del presente contrato.

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 FONACOT"**.

“EL INSTITUTO FONACOT” 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 FONACOT”**.

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 contrato, cumpla con lo dispuesto en el Reglamento de la **“LAASSP”** y no se encuentre en los supuestos de impedimento previstos en la **“LAASSP”.**

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

“EL PROVEEDOR” será responsable en caso de infringir patentes, marcas o viole otros registros de derechos de propiedad industrial a nivel nacional e internacional, con motivo del cumplimiento de las obligaciones del presente contrato, por lo que se obliga a responder personal e ilimitadamente de los daños y perjuicios que pudiera causar a **“EL INSTITUTO FONACOT”** o a terceros.

De presentarse alguna reclamación en contra de **“EL INSTITUTO FONACOT”**, por cualquiera de las causas antes mencionadas, **“EL PROVEEDOR”**, se obliga a salvaguardar los derechos e intereses de **“EL INSTITUTO FONACOT”** de cualquier controversia, liberándola de toda responsabilidad de carácter civil, penal, mercantil, fiscal o de cualquier otra índole, sacándola en paz y a salvo.

En caso de que **“EL INSTITUTO FONACOT”** tuviese que erogar recursos por cualquiera de estos conceptos, **“EL PROVEEDOR”** se obliga a reembolsar de manera inmediata los recursos erogados por aquella.

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, 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 **"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 Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 102, fracción II, de su Reglamento, **"EL INSTITUTO FONACOT"** 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 contrato podrá continuar produciendo todos sus efectos legales, si **"EL INSTITUTO FONACOT"** así lo determina; y en caso que subsistan los supuestos que dieron origen a la suspensión, se podrá iniciar la terminación anticipada del contrato, conforme lo dispuesto en la cláusula siguiente.

VIGÉSIMA TERCERA. TERMINACIÓN ANTICIPADA DEL CONTRATO.

"EL INSTITUTO FONACOT" cuando concurran razones de interés general, o bien, cuando por causas justificadas se extinga la necesidad de requerir 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 FONACOT"**, o se determine la nulidad total o parcial 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 FONACOT"**, ello con independencia de lo establecido en la cláusula que antecede.

Cuando **"EL INSTITUTO FONACOT"** determine dar por terminado anticipadamente el contrato, lo notificará a **"EL PROVEEDOR"** hasta con 30 (treinta) días naturales anteriores al hecho, debiendo sustentarlo en un dictamen que precise las razones o las causas justificadas que le dieron origen a la misma, una vez notificada la terminación anticipada, se extinguirá el contrato, lo que dará lugar a formalizar el finiquito entre las partes.

En el finiquito se harán constar los pagos que, en su caso, deba efectuar **"EL INSTITUTO FONACOT"** por concepto de los servicios prestados hasta el momento de la terminación anticipada, además, en su caso, pactará en el mismo el reembolso al proveedor de los gastos no recuperables en que haya incurrido, siempre que estos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente contrato.

VIGÉSIMA CUARTA. RESCISIÓN.

"EL INSTITUTO FONACOT" 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 contrato, sin contar con la conformidad previa y por escrito de **"EL INSTITUTO FONACOT"**;
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;
i) No entregar dentro de los 10 (diez) días naturales siguientes a la fecha de firma del presente contrato, la garantía de cumplimiento del mismo;
j) Cuando la suma de las penas convencionales exceda el monto total de la garantía de cumplimiento del contrato;
k) Cuando la suma de las deducciones al pago, excedan el límite máximo establecido para las deducciones;
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 FONACOT"** en los términos de lo dispuesto en la **CLÁUSULA VIGÉSIMA PRIMERA DE CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES** del presente instrumento jurídico;
m) Impedir el desempeño normal de labores de **"EL INSTITUTO FONACOT";**
n) Cambiar su nacionalidad por otra e invocar la protección de su gobierno contra reclamaciones y órdenes de **"EL INSTITUTO FONACOT"**, cuando sea extranjero, y
o) No presentar la opinión favorable de sus obligaciones fiscales durante la vigencia del presente contrato
p) Incumplir cualquier obligación distinta de las anteriores y derivadas del presente contrato.

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

Transcurrido dicho término **"INSTITUTO FONACOT"**, en un plazo de 10 (diez) días hábiles siguientes, 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 contrato, y comunicará a **"EL PROVEEDOR"** dicha determinación dentro del citado plazo.

Cuando se rescinda el contrato, se formulará el finiquito correspondiente, a efecto de hacer constar los pagos que deba efectuar **"INSTITUTO FONACOT"** por concepto del contrato hasta el momento de rescisión, o los que resulten a cargo de **"EL PROVEEDOR".**

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

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

"EL INSTITUTO FONACOT" podrá determinar no dar por rescindido el 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, **"INSTITUTO FONACOT"** elaborará un dictamen en el cual justifique que los impactos económicos o de operación que se ocasionarían con la rescisión del contrato resultarían más inconvenientes.

De no rescindirse el contrato, **"EL INSTITUTO FONACOT"** 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 FONACOT"** quedará expresamente facultada para optar por exigir el cumplimiento del contrato, o rescindirlo, aplicando las sanciones que procedan.

Si se llevara a cabo la rescisión del 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 FONACOT"**.

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 FONACOT"** 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 FONACOT"**, así como en la ejecución de los servicios.

Para cualquier caso no previsto, **"EL PROVEEDOR"** exime expresamente a **"EL INSTITUTO FONACOT"** 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 FONACOT"** 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 FONACOT"**, **"EL PROVEEDOR"** queda obligado a dar cumplimiento a lo establecido en la presente cláusula.

VIGÉSIMA SEXTA. DISCREPANCIAS.

"LAS PARTES" convienen que, las estipulaciones que se establezcan en este contrato no deberán modificar las condiciones previstas en la convocatoria a la licitación, invitación o solicitud de cotización, y sus juntas de aclaraciones; en caso de discrepancia, prevalecerá lo estipulado en estas, conforme a lo previsto en el artículo 66, párrafo segundo 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.

"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.

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 Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento; Código Civil Federal; Ley Federal de Procedimiento Administrativo, Código Nacional de Procedimientos Civiles y Familiares; 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.

"LAS PARTES" 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 en las fechas especificadas.

POR:
"EL INSTITUTO FONACOT"

NOMBRE	CARGO	R.F.C.
JAZMÍN GARCÍA JUÁREZ	SUBDIRECTORA GENERAL DE ADMINISTRACIÓN	GAJJ830521BY9
RICARDO ORIA ESQUIVEL	SUBDIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	OIER8103266T3
FERNANDO ZEPEDA DELGADILLO	DIRECTOR DE RECURSOS MATERIALES Y SERVICIOS GENERALES	ZEDF7412252J5

POR:
"EL PROVEEDOR"

NOMBRE	R.F.C.
IQSEC, S.A. DE C.V.	IQS0708233C9

Cadena original:

cf10d3eb4b80f1fdd74306ab6e6152f1822b19451b959eba448ba2d0b2beb22b

Firmante: FERNANDO ZEPEDA DELGADILLO
RFC: ZEDF7412252J5

Número de Serie: 00001000000705259722
Fecha de Firma: 14/11/2025 10:53

Certificado:

MIIGSzCCBDOgAwIBAgIUMDAwMDEwMDAwMDA3MDUyNTk3MjIwDQYJKoZIhvcNAQELBQAwggGVMTUwMwYDVQQDDCxBQyBERUwgU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEuMCwGA1UECgwlU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxMjAwBgkqhkiG9w0BCQEWI3NlcnZpY2lvc2FsY29udHJpYnV5ZW50ZUBzYXQuZ29iLm14MSYw
JAYDVQQJDB1Bdi4gSGlkYWxnbyA3NywgQ29sLiBHdWVycmVybzEOMAwGA1UEEQwFMDYzMDAxCzAJBgNVBAYTAk1YMQ0wCwYDVQQIDARDRE1YMRMwEQYDVQQHDApDVUFVSFRFTU9DMRUwEwYDVQQtEwxTQVQ5NzA3
MDFOTjMxXDBaBgkqhkiG9w0BCQITTXJlc3BvbnNhYmxlOiBBRE1JTklTVFJBQ0lPTiBDRU5UUkFMIERFIFNFUlZJQ0lPUyBUUklCVVRBUklPUyBBTCBDT05UUklCVVlFTlRFMB4XDTI0MDIyMDE5NDExOFoXDTI4
MDIyMDE5NDE1OFowgdYxIzAhBgNVBAMTGkZFUk5BTkRPIFpFUEVEQSBERUxHQURJTExPMSMwIQYDVQQpExpGRVJOQU5ETyBaRVBFREEgREVMR0FESUxMTzEjMCEGA1UEChMaRkVSTkFORE8gWkVQRURBIERFTEdB
RElMTE8xCzAJBgNVBAYTAk1YMSMwIQYJKoZIhvcNAQkBFhRhYm9mZXI3NEBob3RtYWlsLmNvbTEWMBQGA1UELRMNWkVERjc0MTIyNTJKNTEbMBkGA1UEBRMSWkVERjc0MTIyNUhERlBMUjA3MIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAx9RcrRK/IWF6ow1WWq1L4/Lzd+fDwNT1e9SZVIPuYKJRCYdN4hOuaZ3UEFPs+PtD1jyShNY/QcXs0Gm+sQaKPi0MM/HAZ0OJ/NhwFfP36q3bSLKwDF5EK22ZWjn9SzxX38ZM
H1kUE5t9KtUZ90AXpa+x5rDRPiuCNbYFxawKSX1761yTuuuD4aBDPvEyPaPX5DQ48YGFCHwzT3887DkjdkCg6Xze/TuU0UG1MtmLTOp2InwXTd3AW1U1jMPrybLSqbXSyFB1Vujpx6A4Dv6Viu5upFxhuIYqHRJb
4n7zoJDAEVH5gGJfxe0uH9/IxvRxGFtCxfpG9VLHgdilRrA0aQIDAQABo08wTTAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwID2DARBglghkgBhvhCAQEEBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwQGCCsGAQUF
BwMCMA0GCSqGSIb3DQEBCwUAA4ICAQC856j0KjNXdxSIRKEnXE1iDMhRQ0Xw7O626oSpLIYqwZ8l8P0H1Vi26/vbR01UR0gE/JvTVc3hrwwcZAPr+F3Mu/DMEYacimybZ7IgAvSM+5taDpH1v3Ac+8XB71ZGQZnB
57RVkiHO8iHDSm6/o4Cv9z9YwaxtGSFlsa0DDSTdw3CpGFJYX/xeKi53gcHUC9xoxEEyykFFWbKkO9lRHnJpn3ky5A6pjmA0SZ2VeZRmtNKQkCfmhQSKWIzgJXH3eOvaTu2mm7L4MLnAVEf1Qaewy2SL5kT2JayfBdCe/D+OqCWnWdTFoZNYbEb4QQ9X/GIFgDqs2g1ZtM3kACNpOjgeHCwSXdc6kLu3LdKZ3tRk7nR2QR3XpaP92BBEEwQdjbZrfhg9tPMRaORJOYsf26zaejkA25nCKVDtYSE1tmio6YnWJG6ajcme69b3xwONgG0n
qm+0/n2D3j9aMyn8ZQPdDmTpO5mJOsjdSoJk6eFbn9eSC5A/CzxVc4m8A0k3QJ0Kicx7ZJdoHucl/qQcqBDIChv7DxJ6UOQy3XNJ/DlWeMzF5YRQsV51mFKzFwnndOtxs0bUzevIGQt9tUdYsmPFJKKjIhWPKQtQ
YaNP/iXuLCkjYlhVF9pYNDqArA0ezdvrHYRHTS99eyD6Xg65HAhyLD37CqrLX8auEuJUS3bVeA==

Firma:

NxwjPHzZEWomOR38NWRU0yWH/JgHUhLYHUYKbQeE3GMgUNZk3+oyqZ3ulrxtFJQ9l2v5p1/5fW0I89NjGtEjYa1Gfhxj0d7LUA9M/1qI2CLfU62xH5gPrvq+GgPp1FkDPOvCZqTQ7EQ4Zn10/x18SNZBJntWZ2ln
sNF9lorm0gQKyVqNKRCoDs38lj/2uAzcaH7ht63S+0F1wiKNozo9QSmwhw6FKuEFEhiBssM5O8b204JLplNWPPKgYI6ixQi45zYc/BrwoWbgR1exV4CFGRcOy5Q6Fd/VkyW7UZRJqUpoxCm+nNhxh5g6h0B6KWgk
M48otISXN5WjvG+ZsrdqSA==

Firmante: JAZMIN GARCIA JUAREZ
RFC: GAJJ830521BY9

Número de Serie: 00001000000703552192
Fecha de Firma: 14/11/2025 14:05

Certificado:

MIIGOTCCBCGgAwIBAgIUMDAwMDEwMDAwMDA3MDM1NTIxOTIwDQYJKoZIhvcNAQELBQAwggGVMTUwMwYDVQQDDCxBQyBERUwgU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEuMCwGA1UECgwlU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxMjAwBgkqhkiG9w0BCQEWI3NlcnZpY2lvc2FsY29udHJpYnV5ZW50ZUBzYXQuZ29iLm14MSYw
JAYDVQQJDB1Bdi4gSGlkYWxnbyA3NywgQ29sLiBHdWVycmVybzEOMAwGA1UEEQwFMDYzMDAxCzAJBgNVBAYTAk1YMQ0wCwYDVQQIDARDRE1YMRMwEQYDVQQHDApDVUFVSFRFTU9DMRUwEwYDVQQtEwxTQVQ5NzA3
MDFOTjMxXDBaBgkqhkiG9w0BCQITTXJlc3BvbnNhYmxlOiBBRE1JTklTVFJBQ0lPTiBDRU5UUkFMIERFIFNFUlZJQ0lPUyBUUklCVVRBUklPUyBBTCBDT05UUklCVVlFTlRFMB4XDTIzMTEyMTA1NDI1MFoXDTI3
MTEyMTA1NDMzMFowgcQxHTAbBgNVBAMTFEpBWk1JTiBHQVJDSUEgSlVBUkVaMR0wGwYDVQQpExRKQVpNSU4gR0FSQ0lBIEpVQVJFWjEdMBsGA1UEChMUSkFaTUlOIEdBUkNJQSBKVUFSRVoxCzAJBgNVBAYTAk1Y
MSMwIQYJKoZIhvcNAQkBFhRqYXp6eV90YUBob3RtYWlsLmNvbTEWMBQGA1UELRMNR0FKSjgzMDUyMUJZOTEbMBkGA1UEBRMSR0FKSjgzMDUyMU1NQ1JSWjA2MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAo2lVNqh+L94GJm7mAcDdGDeV3HLSmNE/Pab6uvzNqnXDK5yMqBpOZO3UEh8qNKtp/KHHvjAIBbwb2ZOfiosd/WQA4bDJmoLBeBveiwTVPwfpiWR0Jn7gfq6LVA/pafTHst1C7vjslc6aMnehpI5BFVW6BzVH
nR+OqJe8esSilNxVvMFtXdRSC/sHg8nFAHpzCT388ZY/oB0T4fE12vltUbAZfsPs6bcsWLkr3PM+1Vg28ep9l0251mWMwxsIw3lVv+Boli79pClgddkxxyj1o5ryqqP9Dbck+bgniFXES5Gt8ip086YTH5Ke5LZd
z6y47mw+Q1YyESexzmkmqYgH0wIDAQABo08wTTAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwID2DARBglghkgBhvhCAQEEBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwQGCCsGAQUFBwMCMA0GCSqGSIb3DQEBCwUA
A4ICAQBehwClt4AtRzYE5ix4DUyNgWUB3mRpmWd0ho4acgGeW6tSMPC2ymdi7eU46VZ4uMXfZ2sLaLOoKB7ZW06gGaGnsFI7aELnA9xmK/9q7vn6q4OmPnzWTJ+1IlHdBFp6vpGtnq+6B4efHo3vJBygvFzAsy7g
rc1O1YCr4GueCrrE292Z+epybTaV5zv29t1NpICi1r3oc6je7+ZqXUX6sM9Q+r4J1Nkn1l8dFdZGyTmC9M1vlQcEB317gp2CqRfW8kP8Cgng6HrTHdoxcfimR7cvAMdqFLAJsRWeJ533S0Wy0RJKsKK8B8NquNQH
/M+Wwpyl83JyVIdiiq9cGHJpGNXQuupTQmM2JoVzlvg6PqM4KXpRrQiXQCq257thCrgwwAspwlO+UUHJPq+gpPrc2Y7av1DGZRNbtudKRPyxDv9jL4vbUV/2dgb6t79bD0j0adbSnJBpgIQ+3VCJGwAWyaCz4y1m
RoOLPUfPoy4vKTTnXvctifIlUhuO/u3+YaXYSoQTN4aCK23tGexe6UBSA6gYtMbcZpMMYmiCexmWp9yQJkXv8InqtyAZJsN3Gbr14JYzp8cW0g1jE3nDRn7AZ4BIHIomgV/wX7ynmBPHX/mLk5GzENRHqJPc39ty
FaGkCznavGKGqfO6cA0YNBDM+qG+dB6A0deXbxSQtr41Ln1QPw==

Firma:

LVIMHd35x6ebDbbTc0UHFUuHilDChTvqtjK/wvBz6m2VCqVU+51qpE/+xexmnggrjO9R6wfwxMM4J3BYE9zZl6yKxbjTkXZ2UTucbGPaY4C2u6+ffTpIA29xZJsCEyi5I4L9I6ZL5N+N0O4Dvptr9sdNLX1sG6g/
0lFkwpZBl6KcMfF/oTPhHmV4yNlL4oZvvyAbVUwG9pv8PEr41F+VjzakMTAEqjDyy9MEEpdZ/A4NepE3bx86VV7SAF4GyGT9/bwaROWi06yueynQaw2FNsw7JvBjQty96qB//LMgF/lBlvXdu7kiWAzlHVdDT6b7
H7LAOqesRRGVsCy0s29t7A==

Firmante: RICARDO ORIA ESQUIVEL
RFC: OIER8103266T3

Número de Serie: 00001000000705523257
Fecha de Firma: 14/11/2025 14:46

Certificado:

MIIGNjCCBB6gAwIBAgIUMDAwMDEwMDAwMDA3MDU1MjMyNTcwDQYJKoZIhvcNAQELBQAwggGVMTUwMwYDVQQDDCxBQyBERUwgU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEuMCwGA1UECgwlU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxMjAwBgkqhkiG9w0BCQEWI3NlcnZpY2lvc2FsY29udHJpYnV5ZW50ZUBzYXQuZ29iLm14MSYw
JAYDVQQJDB1Bdi4gSGlkYWxnbyA3NywgQ29sLiBHdWVycmVybzEOMAwGA1UEEQwFMDYzMDAxCzAJBgNVBAYTAk1YMQ0wCwYDVQQIDARDRE1YMRMwEQYDVQQHDApDVUFVSFRFTU9DMRUwEwYDVQQtEwxTQVQ5NzA3
MDFOTjMxXDBaBgkqhkiG9w0BCQITTXJlc3BvbnNhYmxlOiBBRE1JTklTVFJBQ0lPTiBDRU5UUkFMIERFIFNFUlZJQ0lPUyBUUklCVVRBUklPUyBBTCBDT05UUklCVVlFTlRFMB4XDTI0MDMwNDE1NDcyMFoXDTI4
MDMwNDE1NDgwMFowgcExHjAcBgNVBAMTFVJJQ0FSRE8gT1JJQSBFU1FVSVZFTDEeMBwGA1UEKRMVUklDQVJETyBPUklBIEVTUVVJVkVMMR4wHAYDVQQKExVSSUNBUkRPIE9SSUEgRVNRVUlWRUwxCzAJBgNVBAYT
Ak1YMR0wGwYJKoZIhvcNAQkBFg5yb3JpYUBsaXZlLmNvbTEWMBQGA1UELRMNT0lFUjgxMDMyNjZUMzEbMBkGA1UEBRMST0lFUjgxMDMyNkhERlJTQzA5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
uzUOWR+3OHN6d9ST7GKnTYPxSnxSOvMHX1+IOvo9xRDsY8do2afaaUaOEpzkTjAiK5U7J05jajwtMjLgD+Flsf4yPpQz+JUZm9ub6ayJc2ekwpkaSsC1N2W0MHty1CpClHjZlB5xdaT06ElS8wVXgig5bMpeQZWA
qSlTFh8/0xM6c6Tvma044VFKGA9zIDVvT8Q/xIEhxwM9jf081zF2ekvxci8hMO558XRrjt9UtEe3/W119TbM5gb4qNE5GyWkrq83zsnUQbCu0Is0Mi6x4vsvxtcF9D3aiOhkVXgCELbQ73Rvf5qblKB4K4zHm152
IZkscqcn4L8HidvwvII9ywIDAQABo08wTTAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwID2DARBglghkgBhvhCAQEEBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwQGCCsGAQUFBwMCMA0GCSqGSIb3DQEBCwUAA4IC
AQA1sYINgJSDUY3/eII3oLG2fGTiQpSau1cqTejf5qth6pZtinfQOkTppc/cmfsKvL1nNRqvt4/JqU9YQUonrBk7b4Yz9h68EJ7413FjlXYNHpOS6d19TTUkMOecxtqLpJKpxTLAVJRQ1C45eTB1bD0/IRtcA5Qz
gFOqRILWRduRduh+LUJJSja74czlIoTN2fMf4Yt2+aUmmZy5jkbcuh45FDntonGfTmg7GFNdUAQVBno5SvhpSz1or/pjImV2qd0kyoeOMP1YwqusT228yFvl6mfWiZ7YOA1BlaxNxtrYv7ZNNDnl3DJypGScKC7e
kTftjAJZKAYLbc2RKpKfF8rz0zACLwylupJ7T0LtLsBxp0gN8Qn1WVuP70FEfRvlG8MfzmPIl7F69KU94HcmNOmvj8W+eDM/RJPiXtCLcQUcc8Ff0QXvzYtsohOBRGGlcMEpmQxz3O0UVmFi39lh97py+Larmkzj
Xf/nUoddH84l2bN+uh19HYGChfeIuIvYHfAImCUYNudOClR+IvhvkFKeogYen+OaopF4QGwuBnWEsyyggYSJdHggFgdXjTpYzC8mQZ71hmweX6HMOpoSBjSu0DTZszJfa1AqgZgu0ygVKE9Zeu73A4dCvPGcc9HN
9HtQ9p5vJtCae7KHa9bKKvRpAEdVOcMf/PuO8F6BgsR2jQ==

Firma:

He2P0XIQtbxC/7SU2cn6A4qeT6fKTa+Kr4KwvDE7aFvXGt2rSS4IKf9BWB2yLQhvTOR2I3Tbd8pn9LjxaJMx0lpF1Wq7eeihBd4/Y1ikpWxHP1+PcQ0xdg5VC1L5HSUizIeCUTRDwymQrKvySCWN+zW5Pg6aR8h3
GbH5vDRkgmfMWNg0iVqQw+4YdMWRbFsngoukgQwHpBSFduwB1VNiczxSSert5YWnRDgzknbMZYiSDTjB8ic+9yG+k+ZGNXfHYn37yk0/f3GZcZL2wZNRb64N6cneBZNhKlxzDRRBMSSw5y0TM244OvHcb6klRdMi
9LgoTkaCUrQi0I+g51Xn4A==

Firmante: IQSEC SA DE CV
RFC: IQS0708233C9

Número de Serie: 00001000000700383593
Fecha de Firma: 14/11/2025 15:41

Certificado:

MIIGPDCCBCSgAwIBAgIUMDAwMDEwMDAwMDA3MDAzODM1OTMwDQYJKoZIhvcNAQELBQAwggGVMTUwMwYDVQQDDCxBQyBERUwgU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEuMCwGA1UECgwl
U0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxMjAwBgkqhkiG9w0BCQEWI3NlcnZpY2lvc2FsY29udHJpYnV5ZW50ZUBzYXQuZ29iLm14MSYw
JAYDVQQJDB1Bdi4gSGlkYWxnbyA3NywgQ29sLiBHdWVycmVybzEOMAwGA1UEEQwFMDYzMDAxCzAJBgNVBAYTAk1YMQ0wCwYDVQQIDARDRE1YMRMwEQYDVQQHDApDVUFVSFRFTU9DMRUwEwYDVQQtEwxTQVQ5NzA3
MDFOTjMxXDBaBgkqhkiG9w0BCQITTXJlc3BvbnNhYmxlOiBBRE1JTklTVFJBQ0lPTiBDRU5UUkFMIERFIFNFUlZJQ0lPUyBUUklCVVRBUklPUyBBTCBDT05UUklCVVlFTlRFMB4XDTIzMDYwOTIxNDczNFoXDTI3
MDYwOTIxNDgxNFowgccxFzAVBgNVBAMTDklRU0VDIFNBIERFIENWMRcwFQYDVQQpEw5JUVNFQyBTQSBERSBDVjEXMBUGA1UEChMOSVFTRUMgU0EgREUgQ1YxCzAJBgNVBAYTAk1YMSYwJAYJKoZIhvcNAQkBFhdp
c3JhZWwucXVpcm9zQGdtYWlsLmNvbTElMCMGA1UELRMcSVFTMDcwODIzM0M5IC8gUVVQSTc0MDMxNVU4NTEeMBwGA1UEBRMVIC8gUVVQSTc0MDMxNUhERlJMUzA1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAyu3OwrrOJckYfk6+dQUDHaH1SVKXAg4qdZKuTvqqlC262VWb/DCwswDwapjb8626oaw9wKvm6Vn+8Q47xEf4legWpxXJpbEtEjGH64PiWQeGiPDk73BX/HaenOhKohpZxBT6IbclKLF8e/kCHi2SKTVo
n0CAlLQi4oVgUnnlrljDH3b0nOvGRc4bxESUi5CRqYOUbtb+Cc0viY2lYlydBh0jddFQXF3k8WFQMoBMOWfwmsquBSJS+k9f1tpuhKpht+M5uVzdY23tJQcsHzOW0poJxkYfOowUSlS3mKyCSwGo18PBMcPILIQ7
VE6om4Y1nLaMvpBKO9/3cgWfCDFY7QIDAQABo08wTTAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwID2DARBglghkgBhvhCAQEEBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwQGCCsGAQUFBwMCMA0GCSqGSIb3DQEB
CwUAA4ICAQBLHmjJsmiMKiU4mN4TGGJ4qwtiVPQjD2ERiBAxgpTSZqgGOIqqBKUA3Obfd5dKbrOf/D40aYLPDzCzqilFvO7jxpjlA2oaaXyns6ON7L3O8tpiGNSYtdA92gn1GMd9v5hi1u0b+nSRLIo7b1sc1QP6
pDTFOUtc0MUNbQhzDQaWluR1SsGv3p/Xdj3dVqgfeWpYePCxfun+UbhbPQZYMougO6Mf0qvyHllze/QdSwrOEJ5tRJFR0F/9BNn697P5QxGGN8v8Tfby8XFrYZtweuZCVof1OIyWeqV40hbjN8KjVqtBwlOheT7b
+3YnrVOPA9ZkUdetcCXpbuRucJi0dwXqzbys7OAWeWUySudGaztDouga+DK4QWIeEOv9tp/mr4KawFik1Ko5oV6Ap9WQ8JiTGmpaSPcD5YrTFMt2fcUXbH/nqizKV7NbrbcvFFgtGpKVEM6Y0XC7Cl2fRmiiFI2a
HWJnXEg0Y5r2XlDIer/pSDXxkVVFSZRTzZsdD3MyxeTtvWSIplg9Zb4o1tJTEUm7YbygI4Ln5YaGGqJZlgnzSn3zAehZa6e5Bfr1037kFyI0iRboveqAG4aLf6rXn/ygp2FLY7dN0EWzAwd4krHxll61WqOY9Lt8
314NCxx8l6JxD6oYZ6LbzglpCvm7SmKZGr7WniNugGCm5W2Mk/Fx9w==

Firma:

vQlnklyOjVgIF6OSDhY8DmB2oPlnXvTo7kC12Itx5RVhApltDILUAULXOCvi9IX//nXbhEwdr1v8WILFwqBNXAbIwWbKWCplBsPXzyRysAE30jlFqcDhCKQ6AbBMvvdhGPPKtcuSTurkolOlsjgiTv44vKLyPjar
sDWQWRE7DmQ+9snqvG9VdYMEAnXuk42blEeUdckTgTMkAHdGCLxMxK2/CgeRZ9Ajg1eedUhzAmEhyjsoG4Svt3ZOGJW7ejtDvcS6jjpQZXZnkFo3w78W+NFcnsgP5Pwi8DM7mSwgZVAJmzYYKxe8P4uwe3AqRw+1
DEFyMpdbljYZoEDtR0l39w==

ANEXO I
Anexo Técnico

ANEXO TÉCNICO

SERVICIO ADMINISTRADO DE CIBERSEGURIDAD

TABLADECONTENIDO

1. OBJETIVO

Nombre del proyecto: "SERVICIO ADMINISTRADO DE CIBERSEGURIDAD".

Disponer de los beneficios relacionados con la contratación del "SERVICIO ADMINISTRADO DE CIBERSEGURIDAD", para el Instituto del Fondo Nacional para el Consumo de los Trabajadores "INFONACOT", cumpliendo con los niveles de servicio establecidos en el presente anexo, y que incluya todas las capacidades necesarias para brindar una protección integral de las aplicaciones y sistemas críticos que se utilizan para proporcionar los servicios financieros clave del "INFONACOT" a sus usuarios finales, considerando una cobertura a nivel nacional en todas las sucursales, oficinas regionales y estatales en un esquema 24x7x365.

2. INTRODUCCIÓN

La importancia de tener un "SERVICIO ADMINISTRADO DE CIBERSEGURIDAD" hacia "INFONACOT" es crítica, ya que con este servicio se contará con una protección integral a los activos críticos, los cuales son utilizados para brindar los servicios financieros clave del "INFONACOT" a sus usuarios finales. El diseño de los servicios administrados deberá estar basado en una arquitectura de capas de seguridad que permita al "INFONACOT" tener visibilidad, trazabilidad y protección en contra de incidentes y amenazas avanzadas que día a día son más sofisticadas y difíciles de detectar, considerando proporcionar la protección en por lo menos la capa de borde (perímetro), la capa de red, la capa de aplicación, la capa de datos y la capa de host (servidores y puntos finales).

Por medio del "Servicio Administrado de Ciberseguridad" se podrá dar cumplimiento a los siguientes conceptos:

- **Confidencialidad:** Se asocia con la privacidad de la información; que se tiene que asegurar para los trabajadores que utilicen los servicios del "INFONACOT". Es la cualidad de la información para no ser divulgada a personas o sistemas no autorizados. Se trata básicamente de la propiedad por la que esa información solo resultará accesible con la debida y comprobada autorización.
- **Integridad:** Esto es la certeza de que la información no ha sido alterada de cualquier manera; entendiéndose a su vez que es la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.
- **Disponibilidad:** Que la información que utilicen los trabajadores y usuarios internos dentro de los sistemas del "INFONACOT" sea accesible cuando la necesiten a través de los canales adecuados siguiendo los procesos correctos.

3. ANTECEDENTES

Con el objetivo de que cada uno de los participantes entienda las necesidades y plantee soluciones que garanticen la continuidad de los servicios durante la fase correspondiente a la transición y toma de operación, es preciso dar a conocer los servicios de Seguridad Informática con los que actualmente cuenta el "INFONACOT".

El "INFONACOT" cuenta con servicios de seguridad informática que le han permitido proveer las condiciones adecuadas para asegurar la continuidad operativa y la correcta remediación, control y mitigación de riesgos, a través de herramientas, metodologías y personal especializado de seguridad de la información.

El servicio es provisto en un esquema 24x7x365 dando atención y cumplimiento a niveles de servicio establecidos. Dichos servicios están orientados a la implementación, configuración, re-configuración,

operación, gestión, soporte y mantenimiento de la infraestructura de Seguridad Informática bajo marcos metodológicos, buenas prácticas, procesos internos, evaluaciones periódicas de seguridad, análisis de riesgos y auditorías de cumplimiento.

4. REQUERIMIENTOS DEL SERVICIO

4.1. REQUERIMIENTOS GENERALES:

"EL LICITANTE" deberá contemplar todos los elementos de hardware y software necesarios para el cumplimiento de los requerimientos del "INFONACOT", estos deberán ser parte de su propuesta técnica.

"EL LICITANTE" deberá comprobar que cuenta con personal certificado en las tecnologías que formen parte de su propuesta, dar soporte y mantenimiento, así como contar con al menos un administrador de proyectos certificado como PMP (Project Management Professional) por sus siglas en inglés para el desarrollo y seguimiento en el aprovisionamiento y soporte del componente tecnológico.

"EL LICITANTE" que resulte adjudicado deberá cumplir con los niveles de servicio solicitados para asegurar una correcta operación y disponibilidad en los servicios requeridos en el presente anexo técnico, lo que le permitirá al "INFONACOT" proporcionar a sus usuarios internos y externos una operación ininterrumpida.

"EL LICITANTE" que resulte adjudicado deberá proporcionar la mejora continua y las correcciones que requiera el "INFONACOT" a las políticas de seguridad configuradas en las soluciones tecnológicas que integran el "SERVICIO ADMINISTRADO DE CIBERSEGURIDAD", con base en los resultados obtenidos en el monitoreo continuo.

La totalidad de los componentes tecnológicos de hardware, software, licenciamientos y/o suscripciones propuestas para los servicios, deberán ser nuevos, de uso exclusivo para el proyecto, de línea y de la última generación liberada en México por parte de los fabricantes, no deberán ser remanufacturados, su fin de vida y/o soporte con el fabricante no deberá estar dentro de la vigencia del contrato y deberán cumplir como mínimo con las especificaciones técnicas descritas para cada uno de los servicios.

"EL LICITANTE" deberá considerar cubrir los movimientos necesarios relacionados con cambios de domicilio durante la vigencia del contrato sin costo adicional para el "INFONACOT", para lo cual deberá reubicar la totalidad de infraestructura y componentes materia del presente servicio, de la ubicación en la cual se implementaron a la nueva ubicación indicada por "INFONACOT", el "INFONACOT" en todos los casos de reubicación será el responsable de facilitar las instalaciones, corriente eléctrica y cableado de datos necesario para la puesta en marcha de los servicios.

"EL LICITANTE" deberá ejecutar las actividades necesarias aplicables a cada caso de las que correspondan y a lo solicitado en la implementación de cada servicio, así como ejecutar las pruebas necesarias que aseguren la correcta operación de los servicios reubicados.

"EL LICITANTE" deberá considerar en la modalidad de servicios bajo demanda, la habilitación de nuevos sitios a solicitud del "INFONACOT", considerando para ello las unidades de crecimiento necesarios por cada uno de los servicios requeridos para el nuevo sitio.

4.2. DESCRIPCIÓN GENERAL DEL SERVICIO

Se requiere contar con un nivel de protección conformado por servicios e infraestructura tecnológica de seguridad en capas requerida para habilitar el "Servicio Administrado de Ciberseguridad", así mismo, contar con el respaldo de un equipo de especialistas con herramientas y software especializado para

fortalecer y acelerar la detección de amenazas, comportamientos anómalos, obtener visibilidad en tiempo real del estado de la infraestructura tecnológica, responder de manera ágil y efectiva ante algún evento en detrimento del "INFONACOT", falla o perdida de la continuidad de la operación, así como minimizar el impacto en caso de materializarse un incidente de seguridad de la información, lo anterior deberá ser considerando tanto para las oficinas centrales, estatales y regionales, así como para las sucursales a nivel nacional.

Los módulos que integran el "Servicio Administrado de Ciberseguridad" se enlistan a continuación:

- Servicio Administrado de SOC.
  - Correlación y Gestión de Eventos.
  - Ciberinteligencia.
- Servicio Administrado de Seguridad.
  - Protección contra amenazas avanzadas en servidores y puntos finales.
  - Gestión de cuentas con acceso privilegiado.
  - Filtrado de contenido web.
  - Protección contra fuga de información.
  - Acceso Seguro en el Borde.
- Servicio Administrado de Protección de Aplicativos.
  - Firewall de aplicaciones web.
  - Firewall de base de datos.
- Servicio Administrado de Seguridad Bajo Demanda.
  - Análisis de código estático y dinámico.
  - Protección del Servicio de Verificación de la Credencial para Votar.
- Servicio de Gestión de Seguridad de la Información.

El alcance de la contratación del "SERVICIO ADMINISTRADO DE CIBERSEGURIDAD", deberá considerar el aprovisionamiento, instalación, habilitación, configuración, soporte y mantenimiento los servicios antes mencionados.

El "SERVICIO ADMINISTRADO DE CIBERSEGURIDAD", deberá incluir los módulos y soluciones tecnológicas descritos en las funcionalidades, especificaciones y/o características técnicas, mismos que deberán contar con una cobertura de soporte 24x7x365 (Las 24 horas del día, los 7 días de la semana por los 365 días del año, durante el plazo de cumplimiento para la prestación de los servicios).

5. CARACTERÍSTICAS DEL SERVICIO

5.1. SERVICIO ADMINISTRADO DE SOC

Para poder contar con un nivel de protección mejorado, es necesario contar con el Servicio Administrado de SOC (Centro de Operaciones de Seguridad), a través del cual se deberán realizar por lo menos las siguientes actividades:

1. Monitorear permanente y proactivamente la infraestructura tecnológica de seguridad ofertada por el "LICITANTE" que permita la detección temprana de amenazas, con el objeto de prevenir impactos adversos a la operación del "INFONACOT".
2. Contar con visibilidad de los dispositivos, aplicaciones y sistemas informáticos institucionales que son protegidos y monitoreados por la infraestructura tecnológica de seguridad ofertada por el "LICITANTE", para detectar fallas o mal funcionamiento, perdida de la continuidad y brindar protección a los mismos.

3. Monitorear y recomendar medidas preventivas tales como la actualización e instalación de parches de seguridad de manera continua en los activos críticos, así como estar documentados para ejercer medidas en contra de ataques de día cero.
4. Analizar, establecer y gestionar alertas para su clasificación con base en su criticidad y prioridad conforme al MGSI de "INFONACOT".
5. Gestionar y analizar logs y bitácoras de la actividad en la infraestructura tecnológica para detectar amenazas de forma proactiva.
6. Analizar e informar al "INFONACOT" el origen y causas de los incidentes de seguridad o intrusiones que se susciten, con el objeto de documentarse y erradicar situaciones similares.
7. Realizar de manera constante la evaluación de la infraestructura tecnológica con el objeto de identificar debilidades que pudieran ser explotadas en detrimento de la continuidad de la operación de las aplicaciones y sistemas informáticos institucionales.
8. Ejecutar las acciones de contención y respuesta ante la materialización de un incidente de seguridad informática, para asegurar que el impacto en la continuidad de la operación del "INFONACOT" sea mínimo.

Como parte del Servicio Administrado de SOC, el "LICITANTE" deberá contar con personal especializado en seguridad defensiva (Blue Team), lo que permitirá defender al "INFONACOT" en contra de ataques de manera proactiva.

El principal objetivo del Blue Team será realizar evaluaciones de las distintas amenazas que puedan afectar al "INFONACOT", monitorear los activos sensibles y recomendar planes de actuación para mitigar los riesgos identificados en los análisis de vulnerabilidad ejecutados en los activos del "INFONACOT" estos activos son parte de los servicios que integran el sistema de crédito institucional de "INFONACOT". Además, en casos de incidentes, deberá realizar las tareas de respuesta, trazabilidad de los vectores de ataque, proponer soluciones y establecer medidas de detección para futuros casos.

El "LICITANTE" en conjunto con el ERISC (Equipo de Respuesta a Incidentes de Seguridad en TIC del Instituto), deberán llevar acabo las acciones de preparación, detección, análisis, contención, erradicación, recuperación, y actividades posteriores a los posibles incidentes que se materialicen en el Instituto. Se requiere que "EL LICITANTE" cuente con un procedimiento o metodología definida basada en estándares abiertos como; el NIST (National Institute of Standards and Technology) y/o ISO 27001;2013 (Sistema de Seguridad de la Información) para llevar acabo la gestión de incidentes de seguridad, con el objetivo de asegurar al "INFONACOT" que "EL LICITANTE" cuenta con un protocolo de actuación con actividades bien definidas para la atención y seguimiento de incidentes de seguridad para evitar o contener impactos derivado de intrusiones, ciberamenazas y otra clase de eventos de seguridad, este procedimiento o metodología deberá ser presentada como parte de la propuesta técnica del "LICITANTE".

El equipo de respuesta a incidentes de "EL LICITANTE" deberá permitir responder de manera eficaz a los incidentes de seguridad de la información tanto de forma reactiva como proactiva; así mismo, deberá fomentar la cooperación y la coordinación en la prevención de incidentes, para estimular una reacción rápida a los incidentes y promover el intercambio de información entre diferentes Centros de Operaciones de Seguridad a través de los CSIRT, es decir, deberá de incluir dentro del SOC los canales de comunicación con otros SOC a nivel nacional e internacional.

A fin de garantizar que se cuenta con un Centro de Operaciones de Seguridad reconocido y con las capacidades de brindar los niveles de seguridad que requiere una Institución Financiera, y en apego a lo establecido en el capítulo 2, articulo 3, del 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, publicado el 06 de septiembre de 2021, el Centro de Operaciones de Seguridad (SOC) de "EL LICITANTE" deberá cumplir con las siguientes características:

1. Deberá acreditar experiencia mínima de 3 años de la operación del SOC (Centro de Seguridad con monitoreo) a la fecha de inicio de los servicios.
2. Acreditar que es miembro de un Organismo Internacional, como lo es el FIRST (Global Forum of Incident Response and Security Teams) o CERT (Computer Emergency Response Team) o contar con una comunicación formal con alguna entidad de Centro de Respuesta a Incidentes Cibernéticos, por ejemplo: CERT-MX de la Guardia Nacional.
3. Deberá acreditar que las instalaciones del SOC se encuentran ubicadas en territorio nacional, y son operadas por los recursos humanos del propio licitante y no un servicio de nube operado por un tercero.
4. Acreditar la certificación vigente en la Norma ISO/IEC 27001:2013, otorgada por una entidad certificadora internacional en por lo menos tres procesos relacionados con la operación de su centro de seguridad, relacionados con los servicios ofertados en este Anexo Técnico. Por ejemplo:
    A. Administración y/o Gestión de Incidentes.
    B. Análisis de eventos.
    C. Ciberinteligencia.
    D. Notificación de vulnerabilidades.
    E. Red Team y Blue Team.
5. Deberá contar con un área exclusiva para el monitoreo dentro del centro de seguridad la cual deberá ser independiente de las demás áreas que integran las instalaciones de "EL LICITANTE".
6. Deberá proveer un servicio de operación en un esquema 24x7x365, para los servicios de monitoreo, servicios administrados y respuesta a incidentes.
7. Deberá contar con atención telefónica 24x7x365 a través de la mesa de servicio del Centro de Operaciones de Seguridad, durante la vigencia del contrato y se deberá integrar con la mesa de servicio del "INFONACOT".

El Servicio Administrado de SOC debe considerar lo que establecen las Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento (CNBV/CUOEF) en los siguientes apartados:

- Capítulo IV Administración de riesgos, Sección Primera, Del objeto, Artículo 59, inciso b).
- TÍTULO SEGUNDO, Sección Cuarta, Apartado B, Artículo 79 inciso b) y Fracción II.

5.1.1. Correlación y Gestión de Eventos

El SOC de "EL LICITANTE" deberá contar con las herramientas para realizar un monitoreo continuo que detecte, analice y permita responder en tiempo real ante incidentes provocados por amenazas tradicionales y amenazas avanzadas en la Infraestructura tecnológica, lo que permita centralizar y correlacionar las bitácoras de los diferentes dispositivos de seguridad para notificar y reportar oportunamente actividades sospechosas que pudieran convertirse en incidentes de seguridad. Así mismo, deberá poder integrar fuentes de información de eventos de seguridad (logs) de activos, activos

críticos o servicios críticos que el "INFONACOT" defina, no importando si estos se encuentran on-premise o en plataformas de nube tales como: AWS, Azure, etc.

Las alertas que representen un riesgo a los activos críticos o a la operación del "INFONACOT" deberán ser notificadas al personal designado por el "INFONACOT" por medio de un reporte en el cual se indicará que se detectó una anomalía. Esta deberá ser investigada por el "LICITANTE" y validada por el "INFONACOT" para descartar falsos positivos.

"EL LICITANTE" deberá proporcionar accesos de monitoreo a los tableros de administración de la herramienta de correlación de eventos a personal que el "INFONACOT" designe.

"EL LICITANTE" deberá considerar una arquitectura centralizada on-premise en el Centro de Datos del INFONACOT" para proporcionar este servicio.

"EL LICITANTE" deberá proporcionar al "INFONACOT", listado de equipos y características fiscas, eléctricas y de BTU para el dimensionamiento de requerimientos, así como hacerse cargo de todos los gastos que genere dicha implementación.

La o las herramientas que sean utilizadas por el "EL LICITANTE" para habilitar el servicio de SOC deberán cumplir con las siguientes funcionalidades:

A. En caso de ser requerido, poder recibir información sobre Indicadores de compromiso (IoC) de fuentes externas de inteligencia, con la finalidad de mantener lo más actualizada su base de datos con información de amenazas avanzadas que puedan afectar los activos o aplicativos críticos del "INFONACOT".

B. Deberá permitir acceder a los eventos de seguridad (logs) originales (raw log data), además de contar con información sobre eventos, alarmas e incidentes de seguridad.

C. Deberá poder realizar la colección de eventos de seguridad (logs) sin agentes, con agentes o de manera hibrida.

D. Deberán poder encolar los eventos de seguridad (logs) en caso de que la cantidad recibida sobrepase la capacidad licenciada de eventos de seguridad (logs), para su procesamiento futuro cuando su carga baje.

E. El tablero de administración deberá contar con la posibilidad de agrupar eventos parecidos con fines de verlos de una manera más sencilla y no repetirlos, además de contar con la posibilidad de generar gráficos específicos de tiempo inicial y tiempo final en la que ocurrieron los eventos.

F. Deberán ofrecer un set de políticas predefinidas, entre las que se deberán de considerar como mínimo y de manera enunciativa más no limitativa las siguientes:

    a. Detección de patrones basados en eventos de seguridad (logs) no observados (not observed compound, not observed scheduled).
    b. Detección de patrones anómalos de comportamiento basados en modificaciones a una línea base (base line).
    c. Detección de patrones en amenazas que salen de estándares básicos (whitelisting).
    d. Detección de patrones anómalos de comportamiento basados en estadísticas (Statistical Behavioral Analisys).
    e. Detección de patrones basados en eventos de seguridad (logs) observados (observed logs).
    f. Detección de patrones anómalos de comportamiento basados en tendencias y su análisis (Trend Behavioral Analysis).
    g. Detecciones de patrones basados en señalización especifica (thresholds)

h. Detección de patrones basados en valores unitarios (unique known, and unique not known values).

G. Deberá considerar no solo información de eventos (limited subset), deberá ofrecer también flujos de datos (netflow, jflow, sflow, ipfix, etc.), eventos de seguridad (logs) nativos, etc. para proveer la máxima capacidad de abstracción posible para la detección de amenazas complejas y advanced persistent threats.

H. El tablero de administración deberá permitir contenidos de visualización tales como mapas de calor (heatmaps), mapas de conectividad (connection maps/contextualization maps), indicadores de compromiso (IOC) y configuraciones completas por el cliente para visualizar cualquier tipo de dato que se encuentre procesado en la o las herramientas habilitadoras de este servicio.

5.1.2. CIBERINTELIGENCIA

Como parte del "Servicio Administrado de Ciberseguridad", "EL LICITANTE" deberá de efectuar a través de su SOC y con la herramienta tecnológica que indique en su propuesta técnica, el monitoreo, investigación y protección, en contra de delitos y fraudes informáticos, falsificación de su imagen a través de canales digitales que se puedan estar en contra del "INFONACOT" y sus marcas comerciales en las redes y los sitios web, así como identificar los procesos y los probables responsables de las diferentes conductas delictivas que representen amenazas de seguridad informática para el "INFONACOT", considerando las siguientes actividades:

- Tendrá la capacidad de proporcionar detección de nombres de dominio fraudulentos o sospechosos.
- Proporcionará el monitoreo e identificación de sitios web que hagan phishing y pharming.
- Proporcionará el monitoreo e identificación del nombre del "INFONACOT" y sus marcas comerciales en la Deep y Dark Web.
- Tendrá la capacidad de dar seguimiento de las actividades realizadas por grupos de activistas, hacktivistas y cibercriminales u otros actores en la Internet (deep y dark web).
- Realizará el monitoreo de vulnerabilidades que pudieran afectar a los componentes de la infraestructura tecnológica del "INFONACOT".
- Realizará el monitoreo de cuentas de correo electrónico institucional de usuarios clave dentro del "INFONACOT".
- Identificará el nivel de riesgo o reputación que tienen asociadas las direcciones IP, CIDRs, dominios y subdominios del "INFONACOT".
- Contará con acceso a fuentes de información, al menos: Controladores RAT de Shodan, Google dorking y Geo IP.
- Proveerá informes de amenazas avanzadas conteniendo información sobre los actores, cuáles son sus motivaciones y las Tácticas, Técnicas y Procedimientos (TTP) que utilizan.
- El Servicio deberá analizar, categorizar y contextualizar de forma automática y dinámica toda la información para su uso inmediato. La categorización y contextualización automáticas deben incluir:

  a. Actores de la amenaza.

b. Malware.
c. Indicadores técnicos.
d. Geografías.
e. Tecnologías.
f. Productos.

- Debe incluir servicio de passive DNS.
- El servicio debe contar con acceso a sitios públicos utilizados para compartir información filtrada (data leak) y publicación de credenciales. Asimismo, debe contar con información histórica de estos.

"EL LICITANTE" deberá notificar de manera inmediata al personal designado por el "INFONACOT" en los casos en que se encuentre una amenaza o vulnerabilidad crítica que afecte los activos u operación del "INFONACOT", con la finalidad de definir los siguientes pasos para estar en condiciones de mitigar los posibles impactos.

5.2. Servicio Administrado de Seguridad

5.2.1. Protección contra amenazas avanzadas en servidores y puntos finales

El Servicio de Protección contra Amenazas Avanzadas en Servidores y Puntos Finales deberá tener la capacidad para detectar, aislar y responder en contra de ataques denominados como amenazas avanzadas, ayudando a reducir el tiempo de detección y la optimización de los modelos de respuesta para de esta manera minimizar el impacto de los incidentes de seguridad. El Servicio deberá tener la capacidad de recolectar, inspeccionar y centralizar la información importante que sucede en tiempo real, de tal forma que en el momento o posterior a un ataque informático se pueda prevenir, contener, responder e investigar con la mayor información posible.

El servicio deberá proporcionar visibilidad de la actividad en los servidores y puntos finales, mientras se aplica análisis y automatización para abordar las amenazas avanzadas. Lo anterior deberá ser ejecutado en los servidores con que cuenta el "INFONACOT", tanto on-premise como en las plataformas de Azure y AWS, así como a los puntos finales" en sus diferentes oficinas, sucursales y home Office. El servicio deberá contar con la capacidad de distribuir políticas de control independientemente de la ubicación en donde se encuentre el servidor o el punto final, incluso fuera de la red del "INFONACOT",

"EL LICITANTE" deberá contar con personal especializado para la correcta administración de la herramienta o herramientas propuestas como parte del Servicio, esto lo deberá demostrar a través de certificaciones vigentes por parte del fabricante de la solución propuesta, misma que se debe mantener durante la vigencia del contrato.

El "INFONACOT" para este servicio requiere inicialmente contar con la protección en los servidores de sus centros de datos, servidores en sus plataformas de Nube y en los puntos finales distribuidos en sus diferentes oficinas y sucursales, considerando, en caso de ser necesario, un crecimiento por unidades, con un máximo de crecimiento de acuerdo con lo requerido en la tabla de volumetrías de los servicios.

El servicio deberá ser habilitado a través de una herramienta tecnológica, la cual deberá contar con una consola central de administración que supervise y recopile información de los servidores y puntos finales que se estarán protegiendo, la cual deberá ser accesible desde cualquier equipo de cómputo a través de un navegador web.

La herramienta tecnológica propuesta por "EL LICITANTE" para la habilitación del servicio podrá ser desplegada por medio de la herramienta de distribución de software con que cuenta el "INFONACOT". En los casos en los que no pueda ser realizado el despliegue a través de esta, "EL LICITANTE" deberá realizar la instalación en cada sitio en donde se encuentren las estaciones de trabajo y servidores del "INFONACOT" sin que esto represente un costo adicional.

El servicio deberá ser implementado en la Fase I al inicio del proyecto. Con la finalidad de efectuar una correcta configuración y puesta en marcha tanto del servicio administrado como de las herramientas habilitadoras del servicio, "EL LICITANTE" deberá considerar por lo menos las siguientes actividades.

- Realizar la instalación, configuración y puesta a punto de la herramienta habilitadora del servicio conforme al alcance establecido en el presente anexo técnico para este servicio, así como a las necesidades de operación del "INFONACOT" y de común acuerdo con "EL LICITANTE" adjudicado.
- Definir y entregar el proceso de escalamiento de incidencias y de comunicación de desviaciones de operación y de incidentes/amenazas potencialmente peligrosas.
- Realizar las pruebas de validación de las configuraciones de la herramienta habilitadora para liberar el servicio a producción.

La habilitación del servicio deberá permitirle a "EL LICITANTE" realizar la detección de amenazas avanzadas a través de técnicas basadas en comportamiento e inteligencia de amenazas.

El servicio deberá cumplir con las siguientes funcionalidades técnicas:

- Utilizar tecnología de inteligencia de amenazas (machine learning), indicadores de ataque, protección de exploits e integración de inteligencia para identificar y bloquear malware.
- Poder contar con mapeo de alertas al modelo de MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®).
- Permitir ver el contexto de un incidente a detalle y con datos de inteligencias de amenazas.
- Permitir identificar el panorama general para tener el conocimiento sobre el nivel de amenaza actual y si cambia con el tiempo.
- Integrar la información de detecciones contra los actores que generan la cadena de ataque.
- Permitir investigar si la institución ya sea por país, región o vertical es vulnerable contra atacantes o actores a nivel global.
- Tener la posibilidad de realizar búsquedas personalizadas, que se remontan a 7 días para buscar amenazas de manera proactiva y que los resultados de las consultas se devuelvan en cinco segundos o menos.
- Brindar protección contra fallas silenciosas (que se producen cuando un ataque se desliza a través de las soluciones de seguridad sin que se active ninguna alarma) y que registre todas las actividades de interés de un equipo tanto en tiempo real como después del hecho.
- Recopilar información constantemente en tiempo real, para asegurar que la información mostrada sea siempre la más actual y relevante.
- Poder desarrollar reglas o indicadores que identifican y previenen ataques sin archivos que aprovechan los malos comportamientos y que con el tiempo ajuste y amplíe los indicadores integrados.

- Incluir Indicadores de Ataque por sus siglas IOA, incluso permitir crear reglas de IOA personalizadas en la plataforma.
- Habilitar una consola central de administración.
- Podrá realizar un inventario de aplicaciones y que versiones están instaladas en los equipos.
- Permitir acceso instantáneo al "quién, qué, cuándo, dónde y cómo" de un ataque.
- Integrar una arquitectura basada en la implementación de agentes en los diferentes endpoints y servidores.
- Detener la ejecución de código malicioso, bloquear exploits de día cero, terminar (Kill) procesos y actividades de comando y control.
- Habilitar una solución on-premise mediante la instalación de agentes en en los diferentes endpoints y servidores solicitados por el "INFONACOT", la cual agilice la implementación al no requerir servidores o controladores a instalar. Es decir, que elimine la necesidad de adquirir un hardware adicional para su implementación.
- Prevenir de forma integral contra ataques que usen malware o bien sin uso de malware (malware-free attacks), además que tenga la capacidad de identificar malware conocido; aprendizaje automático para malware desconocido; bloqueo de intentos de explotación; y técnicas de comportamiento de Indicadores de un Ataque (IoA).
- Tener la capacidad de protección aun cuando los equipos no cuenten con conectividad a la consola de administración.
- Tener la capacidad de detener la actividad maliciosa que utiliza aplicaciones legítimas válidas.
- Utilizar diversos métodos de prevención y detección contra el ransomware, incluidos los siguientes:
    a) Bloqueo de ransomware conocido
    b) Bloqueo de Exploits para detener la ejecución y propagación de ransomware a través de vulnerabilidades existentes.
    c) Uso de Machine Learning para la detección de ransomware de día cero.
    d) Uso de Indicadores de ataque (IOA) para identificar y bloquear ransomware desconocido, nuevas categorías de ransomware que no utilizan archivos para cifrar los datos.
- Para la creación de las reglas personalizadas deberá especificar el "tipo de regla" y seleccionar acciones como: operaciones de creación de procesos, creación de archivos, conexión de red y nombre de dominio.
- No deberá requerir la instalación ni la administración de software adicional. Deberá utilizar la misma consola para administrar políticas y acceder a informes.
- Poder configurar las siguientes políticas:
    a) Bloqueo Completo
    b) Sólo lectura, los usuarios sólo tendrán acceso de lectura, pero no de escritura a dispositivos de almacenamiento masivo

c) No ejecución, los usuarios no tendrán la capacidad de ejecutar programas desde el almacenamiento USB, pero aún tendrán la capacidad de copiar los archivos desde el almacenamiento extraíble a una unidad local.

d) Acceso completo: los usuarios tendrán acceso completo al dispositivo USB.

e) Tener la capacidad de crear reglas por clase y excepciones por ID de proveedor, ID de producto o número de serie.

- Poder identificar inmediatamente qué dispositivos se están utilizando a través de un panel y brinde información sobre los procesos ejecutados desde el dispositivo, usuarios y hosts donde el dispositivo fue utilizado.
- Poder crear reglas de firewall, grupos de reglas y políticas para definir con precisión qué tráfico de red está permitido y bloqueado.
- Poder crear reglas individuales que definan el tráfico de red que será permitido o bloqueado.
- Poder crear un grupo de reglas vacío y construirlo, o comenzar con un grupo de reglas preestablecidas, una colección de reglas básicas que puede editar según sus necesidades.
- Los grupos de reglas deberán organizar las reglas para ser fácilmente asignadas a una política de firewall.
- Ofrecer un servicio administrado de cacería de amenazas capaz de detectar intrusiones, actividades maliciosas y adversarios.
- Como parte del servicio deberá buscar de manera proactiva campañas de malware sigilosas y en caso de existir alguna notificar según corresponda.
- El servicio deberá ir más allá de la detección pasiva y automatizada, deberá investigar e incluso responder a indicadores que apunten a ataques. Alertar con recomendaciones de remediación, con un análisis detallado que permita determinar "qué sucedió" y "cómo responder" al incidente.
- Contar con investigaciones retroactivas revisando datos históricos en busca de evidencia de una intrusión. Recopilar artefactos de investigación como direcciones IP, dominios, hashes y otros. Estos artefactos deberán ser cargados a una base de inteligencia propietaria del fabricante y generar alertas en la interfaz de usuario de la plataforma de seguridad ofertada.
- El servicio deberá estar disponible 24x7x365.
- Deberá proporcionar la visibilidad para identificar "quién" y "qué" hay en la red y supervisar todo desde un panel de control para explorar aplicaciones, cuentas y activos utilizando datos históricos y en tiempo real.
- Contar con el acceso a la información sobre la actividad del host, todo a través de la misma consola, sin tener que importar registros adicionales o ejecutar consultas por separado para obtener visibilidad sobre la utilización de dispositivos USB.
- Utilizar el control de acceso basado en roles para asegurarse de que únicamente los administradores apropiados vean y administren las reglas del firewall.
- Permitir que los datos estén disponibles a través de un tablero de control intuitivo y búsqueda en tiempo real.
- Reportar e indicar si existe actividad anómala en la autenticación de usuarios en los equipos de cómputo.

- Informar el total de cuentas de usuario de dominio y locales que han sido detectados en la autenticación de los equipos de cómputo e indicar el estado de cambio de sus contraseñas.
- Mostrar en un tablero la cantidad de cuentas locales y de cuentas de dominio registradas en los puntos finales
- Mostrar en un tablero el tiempo promedio en meses desde que se cambió la contraseña.
- Mostrar en un tablero los detalles de la última conexión por usuario, definiendo el host donde sucedió, la fecha y hora.
- Mostrar un reporte de los intentos fallidos de acceso de cuentas en los puntos finales a manera de identificar ataques de fuerza bruta a cuentas del dominio o locales.
- Permitir el uso de flujos de trabajo, el cual permita configurar acciones automatizadas.

La herramienta habilitadora del servicio deberá cumplir con las siguientes características técnicas:

- Tener capacidades de antivirus de próxima generación.
- Proporcionar el control de dispositivos removibles (USB).
- Contar con capacidades de Firewall Management.
- Tener un sistema de detección y respuesta de puntos finales (EDR por sus siglas en inglés).
- Contar con una herramienta de inventario de equipos conectados al "INFONACOT".
- Soportar los siguientes sistemas operativos:
    - Linux CentOS 7, Linux Redhat Enterprise 6.7, Linux Redhat Enterprise 7.5 / 7.6 / 7.7, Linux Redhat Enterprise 8.5, Linux Ubuntu 18.04, Microsoft Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 10, Windows 11.
- Combinar el sandboxing de malware, la búsqueda de malware y la inteligencia de amenazas en una solución integral. Además, que tenga la capacidad de producir un Indicador de Compromiso (IoC) tanto para la amenaza que encontró como para todas sus variantes conocidas.
- Contar con la certificación de reemplazo de antivirus
- Tener la capacidad de no interferir incluso con otro software de protección del servidor o punto final para la migración transparente.
- Contar con la capacidad de integrarse a una consola tipo SIEM de distintas maneras ya sea vía API y mediante un conector
- La comunicación y transmisión de datos de los agentes deberá utilizar túneles cifrados (SSL/TLS).
- Ofrecer protección de malware sin la necesidad de utilizar firmas de Antivirus.
- Contar con mapeo de alertas al modelo de MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®).
- Soportar las plataformas Windows, Linux y macOS.
- Permitir detectar incidentes automáticamente sin requerir ningún ajuste o configuración antes de estar en pleno funcionamiento.
- Ofrecer la posibilidad de Zero Trust Assessment (ZTA) para determinar el estado del equipo en el "INFONACOT".

- Para las detecciones de dichas reglas de IOA, deberá tener la capacidad de buscar las detecciones provocadas por una regla especifica.
- Proporcionar visibilidad automática a través del uso de dispositivos USB.
- Permitir leer y escribir desde un dispositivo de almacenamiento extraíble, pero evitar la capacidad de ejecución desde el dispositivo.
- Deberá a través del módulo de EDR permitir obtener mayor visibilidad obteniendo acceso al historial de búsqueda y registros de utilización de dispositivos USB.
- La información del dispositivo deberá incluir registros de uso, eventos de cumplimiento y actividades de transferencia de archivos.
- Tener la capacidad de informar automáticamente el tipo de dispositivo conectado con información del fabricante, nombre del producto y número de serie.
- Ofrecer una administración de firewall simple y centralizada, para facilitar la administración y el cumplimiento de las políticas de firewall.
- Ofrecer inventario de qué aplicaciones y las versiones que se están ejecutando para identificar aplicaciones sospechosas.
- Tener la capacidad de identificar todos los dispositivos en la red, incluso si están protegidos o no por la plataforma.
- Tener la capacidad de monitorear cuentas de todos los usuarios activos en la red, con privilegios de administrador, historial de inicio de sesión e información de actualización de contraseña.
- Combinar antivirus de próxima generación (NGAV), detección y respuesta de endpoints (EDR), búsqueda de amenazas administrada 24/7, inteligencia de amenazas e higiene de TI.
- Proporcionar información contextual para todos los sistemas, utilizando cuadros de mando, gráficos y funciones de búsqueda para profundizar en los datos de apoyo. Los resultados deberán correlacionarse con los dispositivos que están en línea, fuera de línea o no conectados a la red corporativa.
- Utilizar la información de la solución de detección y respuesta de endpoints (EDR) para alimentar los datos de búsqueda.
- Tener la capacidad de minimizar el abuso de cuentas privilegiadas monitoreando el uso y creación de credenciales de administrador.
- La herramienta deberá monitorear todos los equipos a través de un sensor ya sea dentro o fuera de la red, en equipos físicos y virtuales.

5.2.2. Gestión de cuentas con acceso privilegiado

El Servicio de Gestión de cuentas con acceso privilegiado permitirá automatizar la administración de contraseñas y sesiones, a efecto de que el "INFONACOT" cuente con un control de acceso seguro, auditorías, alertas y registros para cualquier cuenta con privilegios, ya sean cuentas locales o cuentas de administrador, lo anterior, a efecto de reducir los riesgos de seguridad y prevenir violaciones de datos. El servicio permitirá tener un control sobre los perfiles usuarios privilegiados, además, de proporcionar trazabilidad sobre las actividades que estos realicen en los activos críticos del "INFONACOT".

"EL LICITANTE" deberá considerar la integración de aproximadamente 120 servidores y 60 bases de datos, considerando 20 usuarios de administración de acceso privilegiado, como parte de la solución.

"EL LICITANTE" deberá contar con personal especializado para la atención de eventos y en su caso su remediación, fallas o requerimientos relacionados con la herramienta o herramientas propuestas como parte del Servicio. Lo cual deberá acreditar a través de certificaciones vigentes en la administración de la herramienta propuesta.

"EL LICITANTE" deberá considerar como parte de la operación del Servicio de Gestión de Cuentas con Acceso Privilegiado atender los requerimientos de accesos privilegiados debidamente documentados y autorizados por parte de las áreas operativas del Instituto, así como del responsable o encargado de las funciones de Seguridad de la Información.

"EL LICITANTE" deberá proporcionar el acceso privilegiado al personal autorizado por el Instituto, dando cumplimiento a las políticas, procedimientos y documentos de control definidos en el Marco de Gestión de Seguridad de la Información del "INFONACOT"

El "INFONACOT" para este servicio requiere inicialmente contar con la gestión de cuentas con acceso privilegiado para los usuarios internos, externos y de terceros que accedan a los activos críticos, considerando en caso de ser necesario un crecimiento por unidades, con un máximo de crecimiento de acuerdo con lo requerido en la tabla de volumetrías de los servicios.

"EL LICITANTE" deberá realizar la instalación, migración de las configuraciones con que actualmente opera el servicio, y poner en marcha tanto del servicio administrado como de las herramientas habilitadoras del servicio, considerando por lo menos las siguientes actividades.

- Realizará la instalación, migración de la configuración actual y deberá poner en marcha la herramienta habilitadora del servicio conforme al alcance establecido en el presente anexo técnico para este servicio, así como a las necesidades de operación del "INFONACOT" y de común acuerdo con "EL LICITANTE" adjudicado, considerando un esquema en alta disponibilidad en el Centro de Datos principal.
- Definirá y entregará el proceso de escalamiento de incidencias y de comunicación de desviaciones de operación y de incidentes/amenazas potencialmente peligrosas.
- Realizará las pruebas de validación en las configuraciones de la herramienta habilitadora para la liberación y puesta en marcha del servicio.

El Servicio de Gestión de Cuentas con Acceso Privilegiado deberá facilitar el almacenamiento seguro y la gestión de sesiones para obtener credenciales administrativas, esto para proteger y monitorear los accesos de las principales cuentas privilegiadas de los aplicativos de redes sociales institucionales.

El Servicio de Gestión de Cuentas con Acceso Privilegiado deberá permitir a los administradores u operadores de los servidores del "INFONACOT", realizar sus tareas diarias en un entorno con privilegios mínimos, donde solo se le otorguen derechos de administrador o root a tareas específicas y autorizadas. Gestionar las aplicaciones que podrán ser instaladas o ejecutadas en los servidores y proporcionar pistas de auditoría e informar sobre cambios en las políticas, aplicaciones y archivos de datos críticos.

El Servicio de Gestión de Cuentas con Acceso Privilegiado deberá proporcionar un control de acceso basado en roles, que permita realizar el perfilamiento de privilegios por cada rol, por ejemplo, cuentas de acceso para instaladores, usuarios de monitoreo, usuarios de soporte entre otros.

El Servicio de Gestión de Cuentas con Acceso Privilegiado y/o la herramienta o herramientas propuestas deberán considerar un esquema de Alta Disponibilidad en su arquitectura.

El Servicio de Gestión de Cuentas con Acceso Privilegiado y/o la herramienta o herramientas propuestas como parte del servicio deberán brindar como mínimo las siguientes funcionalidades:

Administración y resguardo de cuentas privilegiadas.

- Contará con una centralización y almacenamiento seguro de las cuentas privilegiadas.
- Permitir rotar las contraseñas de las cuentas privilegiadas de forma programada según la política que establezca la entidad, sin interrumpir el servicio.
- Proporcionará una rotación automática de contraseñas y llaves SSH.
- Contará con flujos de trabajo automatizados para solicitud de cuentas privilegiadas.
- Contará con controles para la solicitud de contraseñas con auditoria y reportes sobre el uso.

Administración de Sesiones Privilegiadas.

- Podrá brindar el monitoreo y grabación de todas las actividades realizadas con las cuentas privilegiadas en sistemas o servicios críticos como Servidores Windows, Linux, Bases de Datos, Bases de datos como servicio, Máquinas virtuales, Sitios Web, Dispositivos de Seguridad, Dispositivos de Red, Aplicaciones, etc.
- Proporcionará la entrega de sesión privilegiada autenticada al dispositivo o servicio destino al usuario solicitante.
- Permitir que los equipos de seguridad vean y eliminen de inmediato las sesiones privilegiadas no autorizadas directamente desde la consola de la solución
- Evitará mostrar las contraseñas privilegiadas a los usuarios.
- Ofrecer opciones de supervisión y grabación que permitan observar las sesiones privilegiadas en tiempo real, suspender automáticamente y finalizar de forma remota las sesiones sospechosas, así como mantener un registro de auditoría exhaustivo y rastreable de la actividad del usuario privilegiado
- Llevará un registro de comandos, o teclas presionadas por el usuario en las sesiones.
- Podrá prevenir el acceso directo a los sistemas críticos, ofreciendo un puente entre los usuarios y los dispositivos (aislamiento).

Control de Acceso a las Identidades privilegiadas (MFA y SSO):

- La herramienta o herramientas propuestas como parte del servicio deberán soportar al menos la autenticación de los usuarios utilizando múltiples factores de autenticación, incluyendo:
- Autenticar a los usuarios contra Active Directory.
- Código QR propio.
- Código OTP vía SMS enviado por la propia solución.
- Código OTP vía E-mail enviado por la propia solución.
- Notificaciones push a dispositivos móviles enviado por la propia solución.

- Tokens de terceros en cumplimiento con FIDO2.
- Autenticación biométrica de dispositivos como Windows Hello y Apple Touch ID.
- Soportará autenticación adaptable al contexto y riesgo calculado por la plataforma para cada usuario.
- Tendrá capacidad de incluir al portal de usuario otras aplicaciones para su protección con MFA y SSO.
- Deberá tener integración con otras soluciones de autenticación que soporten:
    - RADIUS.
    - PKI.
    - SAML.
    - OpenID Connect (OIDC).

Tecnologías soportadas:

- La herramienta o herramientas propuestas como parte del servicio deberán tener la capacidad de administrar y soportadar diferentes tecnologías, entre las cuales deberán encontrarse por lo menos las plataformas:
    - *Sistemas Operativos:* AIX 7200-03-02, Linux CentOS 7, Linux Red Hat Enterprise Linux (RHEL), Linux Ubuntu, Microsoft Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022.
        - *Bases de datos:* Microsoft SQL Server, Oracle, SAP Hana, MongoDB, MySQL PostgreSQL
        - *Dispositivos de red:* Cisco, Juniper, CheckPoint, Fortinet, F5.
        - *Dispositivos de Seguridad: Juniper, CheckPoint GaiA, CISCO ASA, CISCO ISE.*
        - *Aplicaciones:* SAP.
        - *Entornos de nube con los que actualmente opera el "INFONACOT".*
        - *Directorios:* Microsoft.
        - *Entornos Virtuales:* VMWare, vCenter y ESX.
        - *Interfaces genéricas:* SSH/Telnet, Web, PuTTY, RDP.

Administración general de la solución

- El Servicio deberá proporcionar una administración centralizada a través de un portal web
- Proporcionar una interfaz web donde se puedan identificar fallos, inconsistencias o problemas en asignación roles, permisos o incumplimientos de las políticas de contraseñas
- Realizar el descubrimiento y la clasificación de cuentas privilegiadas y grupos de seguridad.
- La herramienta o herramientas propuestas como parte del servicio deberán estar protegidas por múltiples factores de autenticación adaptable, al contexto basado en el riesgo determinado por geolocalización y horarios de autenticación; esta funcionalidad debe ser proporcionada por

el mismo fabricante, considerando al menos dos de las siguientes; contraseña, código QR, OTP, Notificación Push al móvil con validación biométrica, código enviado al correo electrónico, código enviado por SMS.

- Podrá manejar los controles de acceso basado en roles mediante la administración de grupos de usuarios de Directorio Activo o LDAP, además de automatizar los procesos de aprobación para el aprovisionamiento y des aprovisionamiento de cuentas privilegiadas.
- Utilizar una API basada en REST para conectarse con otras aplicaciones y sistemas, independientemente de lo que desee hacer o en qué idioma estén escritas las aplicaciones
- Administrar cuentas privilegiadas y sus credenciales on-premise y en la nube para instancias: Windows, Linux, IOS, Privilegiadas, Claves compartidas, Administrador local, Administradores temporales, de servicio, Secure Shell (SSH), Administrador de aplicaciones, cuentas de base de datos.
- Permitir un tiempo de retención mínimo y máximo dependiendo de las necesidades de la entidad.
- Contará con interfaz para programadores (API) y de esta forma permita conectarse a otras aplicaciones o sistemas para la automatización de actividades administrativas, entre otras opciones.

Seguridad

- La herramienta o herramientas propuestas como parte del servicio deberán tener la capacidad de cifrar todos los datos, las comunicaciones y conexiones usando algoritmos de cifrado fuertes
- La solución, debe cumplir con cifrado FIPS 140-2 y la ISO27001, así mismo contar con un cifrado completo de disco en AES
- Permitirá que ciertos administradores no puedan visualizar las contraseñas que son controladas por otros departamentos de la compañía, como por ejemplo que los administradores de Windows Server no puedan visualizar las contraseñas ni accesos a instancias de bases de datos SQL Server. Esto es para garantizar la separación de roles lo más posible para evitar el uso indebido de las cuentas privilegiadas protegidas por la solución.
- Permitirá que los administradores de la solución no tengan acceso a las contraseñas almacenadas si así se define por el negocio.

Arquitectura

- El servicio deberá ofrecerse en una arquitectura On-premise.
- Podrá realizar las tareas de gestión de cuentas con acceso privilegiado sin la necesidad de que se instalen agentes en los dispositivos del centro de datos.
- Deberá ser modular y escalable para adaptarse a crecimientos de utilización o de inclusión de más plataformas o aplicaciones.
- Capacidad de permitir una alta disponibilidad (24x7x365) y redundancia en caso de fallas en hardware, aplicación, falla de datos o desastres catastróficos (incluyendo un modelo Activo - Activo).

- Capacidad de implementarse en modo transparente para que no sea necesario realizar cambios en los flujos de trabajo de los usuarios. Actuar como una puerta de enlace proxy que funcione como un enrutador en la red, invisible para el usuario y el servidor.

Integraciones con otros sistemas:

- Podrá integrarse con los directorios LDAP para administración de usuarios (Active Directory).
- Podrá integrarse con la solución SIEM para envió de eventos, alertas y recepción de eventos que ocurren en los sistemas administrados.
- Deberá soportar y en caso de requerirse se habilitará sin costo para el "INFONACOT" integración con servidores de correo SMTP para envío de notificaciones por correo electrónico.
- Soportar conexión automática a dispositivos Windows, UNIX/LINUX, bases de datos, páginas web, dispositivos de comunicaciones, etc.

Análisis de amenazas y comportamiento

- Proporcionar análisis y alertas de actividad maliciosa de acceso privilegiado y permitir detectar, alertar y responder a actividades privilegiadas anómalas que puedan indicar que hay un ataque en curso.
- Capacidad de realizar el análisis de amenazas y alertas que recopilará y analizará de entornos locales, en la nube o híbridos, que contengan el mayor riesgo de daño.
- Este componente deberá contener un motor de análisis que aproveche el modelado estadístico, el aprendizaje automático, y los algoritmos determinados para detectar actividad maliciosa, de manera tal que suspenda o finalice de forma remota las sesiones para permitir que los equipos de seguridad pongan en cuarentena o finalicen inmediatamente las sesiones privilegiadas de alto riesgo.
- Este componente deberá utilizar algoritmos de aprendizaje automático para examinar patrones típicos de usuarios privilegiados individuales, cuentas privilegiadas y actividades del sistema para determinar una línea base de "comportamiento normal".
- Crear perfiles de comportamiento del usuario basados en la actividad de la cuenta privilegiada y utilizarlos como base para identificar actividades sospechosas en el entorno, que incluyen:
  - Datos de registro (Log):
    - Hora de Login
    - Sistemas y aplicaciones típicas accedidas por el usuario.
  - Datos de sesiones:
    - Actividades realizadas por el usuario.
    - Características del movimiento del "mouse".
    - Análisis de dinámica de pulsaciones de teclas.
    - Detección de inicio de sesión programadas que se ejecutan desde script.
    - Detección de inicios de sesión repetida en el tiempo entre ocurrencias.

- Agrupación de similitudes de comportamiento en sesiones con otros usuarios (agrupar por sistema Host, horas de inicio de sesión, duración de sesión, protocolo utilizado, política utilizada, sistema destino).

Características para generación de reportes.

- Generará reportes de forma periódica, bajo demanda o en forma programada.
- Generará reportes detallados y programados con la siguiente información:
  - Usuario
  - Cuenta
  - Activo
  - Cambios de configuración
  - Informes principales
  - Informes por conexión
  - Informes del estado del sistema

- Podrá exportar los reportes utilizando, al menos en CSV.
- Contará con la capacidad de personalizar reportes.
- Podrá restringir el acceso a los reportes de auditoría (y a la configuración de dichos reportes) solo para personal de auditoría.
- Podrá reproducir las sesiones grabadas para propósitos de Análisis Forense.
- Generar reportes de todos los cambios administrativos en el sistema, accesos al sistema, cambios de passwords, intentos inválidos de login y auditoria.
- Brindar reportes del monitoreo de la actividad de los usuarios con prestaciones como: drag-and-drop.
- Generar reportes del registro de la actividad del usuario como: tiempo de inicio de sesión, errores de autenticación, cambios de contraseña, ubicación y dispositivo o navegador usado.
- Proporcionar registros de eventos de seguridad y estos registros deben ser exportables en un formato legible (syslog) para ser enviados a la solución de centralización de registros SIEM.

Características de flujos de trabajo

- La herramienta o herramientas propuestas como parte del servicio deberán contar con la capacidad de soportar controles duales, es decir, deberá contar con hasta 2 niveles de aprobaciones con múltiples aprobadores en cada nivel; de forma tal que cuando un usuario solicite acceso a un servidor/dispositivo, uno de los múltiples aprobadores de cada nivel deba autorizar dicho acceso.
- Tendrá la capacidad de que un usuario pueda solicitar el uso de una cuenta privilegiada especificando una fecha y hora determinados.

Configuración y políticas de contraseñas:

- Capacidad de establecer políticas en las que se pueda especificar una longitud mínima de caracteres de contraseña y complejidad para las cuentas que se resguarden en la solución.
- Proporcionar políticas de contraseña configurables, que permitan características de contraseña segura, complejidad y fecha de vencimiento que se puedan aplicar las diferentes aplicaciones integradas.
- Capacidad de contar con el historial de contraseñas,
- Capacidad de aplicar diferentes políticas por la línea de negocio cuando el tipo de dispositivo es el mismo.
- Enviar correos electrónicos de notificación basado en permisos administrativos:
    - Administrador de dispositivos
    - Administrador de operaciones
    - Propietario de la partición (si no hay ninguno, se envía al Administrador de activos)
    - Administrador de Políticas de Seguridad
- Capacidad de cambiar las contraseñas automáticamente cada determinada cantidad de días, meses o años con base en políticas configuradas en la solución sin depender de agentes instalados en los sistemas destino.
- Cambiar automáticamente la contraseña de una cuenta que acaba de ser definida en el sistema.
- Permitir compartir contraseñas temporales de forma segura dentro de la Organización y los equipos.

Conexión a sistemas destino

- La herramienta o herramientas propuestas como parte del servicio deberán poder ampliar las capacidades de los sistemas UNIX, Linux y Mac para unirse de forma transparente a Active Directory e integrar identidades Unix con cuentas de Windows de Active Directory.
- Capacidad para limitar la línea de comandos y el acceso excesivo para superusuario/cuentas privilegiadas (cuentas raíz con permisos elevados).

Monitoreo y auditoría de sesiones privilegiadas

- La herramienta o herramientas propuestas como parte del servicio deberán tener la capacidad de asegurar responsabilidad personal cuando se abre una sesión privilegiada con una cuenta compartida, de forma que se pueda diferenciar que persona hace uso de una cuenta compartida o genérica, cuándo la utiliza y las actividades que realiza.
- Deberá contar con la capacidad de integrarse a sistemas de Ticketing/Help Desk.
- Deberá contar con la capacidad de hacer búsquedas de comandos privilegiados dentro de las grabaciones de video.
- Deberá poder visualizar las sesiones activas en un momento determinado en tiempo real.

- Capacidad de búsqueda para facilitar la navegación de las sesiones grabadas, tanto por líneas de comandos y video.
- Deberá contar con la capacidad de comprimir las sesiones y sin impactar en la calidad de video.
- Limitar el acceso según las ubicaciones geográficas
- Mantener una trazabilidad completa del uso de la cuenta privilegiada para el análisis forense.

Aislamiento de los usuarios y los sistemas destino.

- La herramienta o herramientas propuestas como parte del servicio deberán funcionar como un puente entre los usuarios finales y los dispositivos administrados. La conexión deberá establecerse desde uno de los componentes de la solución hacia los dispositivos destino y no desde la máquina del usuario que solicita la sesión.
- Deberá ejecutar los programas o clientes de conexión necesarios para la conexión en uno de sus componentes, para evitar que el usuario instale los programas necesarios para la conexión.
- Deberá configurar accesos Just-In-Time a cuentas que no tienen permisos acceder a ciertos servidores.

5.2.3. Filtrado de contenido web

El Servicio de Filtrado de Contenido Web deberá permitir el establecimiento de políticas y controles granulares para la inspección del tráfico que los usuarios del "INFONACOT" generan hacia y desde Internet no importando si estos se encuentran dentro de la red Institucional o fuera de ella. Y de esta manera tener la capacidad de brindar protección a los usuarios (incluso a los usuarios remotos) en contra de sitios web maliciosos o inapropiados, así mismo, permitirá la identificación de amenazas maliciosas, permitiendo filtrarlas, eliminarlas o bloquearlas con el objeto de proteger al usuario de un robo o fuga de información, perdida de datos que puedan poner en riesgo los activos críticos de "INFONACOT".

Por medio del Servicio de Filtrado de Contenido Web se deberá realizar el monitoreo de la transferencia de información en búsqueda de amenazas desde y hacia Internet. Se deberá realizar el monitoreo del uso de aplicaciones en Internet por los usuarios. Así como, la generación de reportes, sobre incidentes detectados, violación de políticas y estadísticas sobre el uso que los usuarios hacen de aplicaciones en Internet.

El "INFONACOT" para servicio requiere inicialmente contar con la protección de navegación y filtrado web en todos los puntos finales distribuidos en sus diferentes oficinas, considerando en caso de ser necesario un crecimiento por unidades, con un máximo de crecimiento de acuerdo con lo requerido en la tabla de volumetría de los servicios.

La herramienta tecnológica propuesta por "EL LICITANTE" para la habilitación del servicio podrá ser desplegada por medio de la herramienta de distribución de software con que cuenta el "INFONACOT". En los casos en los que no pueda ser realizado el despliegue a través de esta, "EL LICITANTE" deberá realizar la instalación en cada sitio en donde se encuentren las estaciones de trabajo sin que esto represente un costo adicional para el "INFONACOT".

"EL LICITANTE" deberá contar con personal especializado en la tecnología propuesta, para la atención de eventos y en su caso su remediación, fallas o requerimientos relacionados con la misma. Lo cual deberá demostrar mediante presentación de certificaciones vigentes en la administración de la solución propuesta.

El Servicio de Filtrado de Contenido Web deberá cumplir con las siguientes características y funcionalidades:

- El servicio deberá permitir realizar el filtrado de contenido web basado en las políticas de navegación establecidas por el INFONACOT.
- El servicio deberá poder filtrar mediante categorías, el acceso a sitios web, combinándolo con grupos, usuarios, departamentos, ubicación, intervalos de tiempo y cuotas de navegación.
- El servicio deberá asegurar y proteger el flujo de información que se transmite a través del punto de conexión entre el "INFONACOT" e Internet.
- El servicio deberá entregarse en modalidad on-premise, considerando la instalación de agentes en los equipos de cómputo de los usuarios finales.
- La herramienta o herramientas propuestas como parte del servicio deberán tener la capacidad de brindar visibilidad y manejo de tráfico cifrado SSL/TLS con características y funcionalidades para filtrar y soportar al menos las versiones de TLS siguientes: TLS 1.0, TLS 1.1, TLS 1.2 y TLS 1.3.
- Tener la capacidad de bloquear la carga y descarga de cierto tipo de archivos, por ejemplo: EXE, RAR, PKG, XLS, PDF, entre otros.
- Por medio del servicio se deberá generar un reporte que permita identificar cuáles son las aplicaciones Web más utilizadas por los usuarios.
- El servicio deberá proporcionar una consola de administración centralizada, para creación de políticas locales que puedan ser distribuidas globalmente en todos los sitios con enlace a Internet, a través de un esquema de jerarquías que incluyan políticas maestras, a nivel de usuario, grupo o departamento.
- La herramienta o herramientas propuestas como parte del servicio deberán contar con la capacidad de integrarse con un Directorio Activo para tener acceso a usuarios, grupos y departamentos, a fin de poder aplicar políticas granulares.
- Por medio del servicio se deberá poder crear reglas para controlar el acceso a ciertas aplicaciones, como redes sociales.
- Contar con la capacidad de crear reglas que disminuyan la pérdida de productividad, así como la fuga de información sensible, mediante el control en aplicaciones de webmail (gmail, outlook, yahoo).
- Tener la capacidad de bloquear el acceso correo electrónico de dominios externos.
- Permitir la creación de categorías personalizadas.
- Soportar la creación y el mantenimiento de categorías, políticas de filtrado de URL a través de un API.
- Proporcionar un mecanismo para bloquear el acceso Web a destinos alojados en ciertos países. Este bloqueo debe configurarse simplemente seleccionando los países que desea bloquear.

- Para las páginas de bloqueo, la herramienta o herramientas propuestas como parte del servicio deberá admitir la redirección a cualquier URL personalizada, que se envía como parámetros en esta URL variables como: acción, categoría de URL, tipo de directiva, motivo de bloqueo, URL y usuario.
- Tener la capacidad de bloquear nubes de almacenamiento no autorizadas.
- Poder crear reglas para controlar el acceso a aplicaciones.
- Proporcionar protección antivirus y antimalware basada en firmas de archivos. Esta protección deberá realizarse para su descarga y carga, y el fabricante deberá actualizar constantemente la base de datos de dichas firmas.
- El servicio deberá proporcionar protección contra amenazas avanzadas en la navegación web, utilizando análisis estáticos basados en la reputación del dominio, el origen, la antigüedad del dominio entre otras variables, y un análisis dinámico del contenido web del 100% de las solicitudes realizadas con el fin de detectar riesgos potenciales para los usuarios, como la inyección maliciosa de JavaScript, las firmas de robo de cookies XSS, contenido activo malintencionado, contenido ActiveX vulnerable, phishing y mucho más.
- La herramienta o herramientas propuestas como parte del servicio deberá tener la capacidad de consumir los datos de inteligencia de amenazas de la herramienta de protección contra amenazas avanzadas para servidores y puntos finales para brindar una protección más sólida y una mayor visibilidad.
- Permitir la generación de registros de acceso detallados de usuarios web, aplicaciones, bloqueos de seguridad y accesos o bloqueo de aplicaciones.
- Contar con la posibilidad de controlar el tráfico FTP, tanto nativo como FTP sobre HTTP.
- La consola de administración centralizada deberá tener acceso directo a los registros y deberá permitir la generación automática de reportes y su distribución por correo electrónico.
- La herramienta o herramientas propuestas como parte del servicio deberán integrarse de forma nativa y enviar registros en tiempo real a plataformas de gestión de eventos e información de seguridad (SIEM) como por ejemplo Splunk o IBM Qradar o MS Sentinel u otros.
- El agente de la herramienta o herramientas propuestas como parte del servicio deberá contar con la capacidad de solicitar una contraseña para deshabilitar el servicio o desinstalar el agente.
- El agente deberá contar con la opción de desplegar notificaciones al usuario.
- El agente deberá ofrecer soporte al sistema operativo Windows, Linux, MAC OS, Android y IOS.
- La herramienta o herramientas propuestas como parte del servicio deberán contar con un módulo de firewall que permite la creación de políticas utilizando destino, protocolo udp/tcp y puerto.
- Soportar crear reglas con IP de destino, subredes o direcciones completas (FQDN).
- Soportar la creación de políticas de Firewall bloqueando el acceso a destinos en países específicos, para todos los protocolos, no solo para la Web.
- El firewall deberá tener capacidad de inspección en la capa 7, haciendo uso de la tecnología deep Packet Inspection (DPI), o similar que ofrezca el mismo caso de uso, para identificar en los primeros paquetes la aplicación que se está utilizando

- La herramienta o herramientas propuestas como parte del servicio deberán identificar aplicaciones como SSH, RDP, Base de datos, DNS sobre HTTPS, Google DNS, Cloudflare DNS, FTP, NFS, NetBIOS, SNMP, P2P BitTorrent, WhatsApp entre otras utilizando DPI (Deep Packet Inspection) independientemente de si están utilizando o no puertos estándar de sus protocolos.
- El firewall de la herramienta o herramientas propuestas como parte del servicio deberán soportar la creación de políticas de API.
- La herramienta o herramientas propuestas como parte del servicio deberán tener la capacidad de crear políticas específicas granulares para la protección de DNS.
- La herramienta o herramientas propuestas como parte del servicio deberán tener protección nativa contra ataques de túnel de DNS, lo que permitirá el bloqueo de objetivos maliciosos conocidos y un mecanismo para detectar firmas de ataque utilizando herramientas de túnel de DNS conocidas como dnscat, independientemente del dominio utilizado.
- La herramienta o herramientas propuestas como parte del servicio deberá detectar y redirigir las solicitudes de DNS utilizando DNS sobre HTTPS (DOH) de manera transparente para la aplicación de políticas de DNS, detalladas en los elementos anteriores.
- La herramienta o herramientas propuestas como parte del servicio deberá tener capacidades de Data Loss Prevention las cuales deberán funcionar tanto para aplicaciones que usen protocolo HTTP como HTTPS
- El componente de Data Loss Prevention deberá permitir crear reglas basadas en expresiones regulares para el monitoreo y bloqueo de exfiltración de datos.
- El componente de Data Loss Prevention deberá permitir crear reglas basadas en palabras o frases.
- El componente de Data Loss Prevention deberá permitir bloquear la exfiltración de contenido tomando en cuenta el tamaño del archivo.
- La herramienta o herramientas propuestas como parte del servicio deberá permitir controlar el tipo de archivos que se pueden subir o descargar.
- El componente de Data Loss Prevention deberá soportar y en caso de requerirse se habilitará sin costo para el "INFONACOT" el analizar imágenes mediante reconocimiento óptico de caracteres.
- Deberá tener integración con la herramienta de protección contra amenazas avanzadas en servidores y puntos finales para tomar acciones de bloqueo en caso de violación de políticas definidas en el componente de Data Loss Prevention.
- La herramienta o herramientas propuestas como parte del servicio deberán permitir identificar y bloquear archivos protegidos por contraseña (ejemplo zip, rar).
- Permitir implementar controles granulares en aplicaciones web como redes sociales y bloquear la posibilidad de compartir información (solo lectura).
- Permitir implementar controles granulares en aplicaciones web como correo electrónico y bloquear la posibilidad de adjuntar archivos.
- Permitir el bloqueo sitios de correo electrónico personal.
- Permitir el bloqueo de acceso a correo electrónico corporativo con dominio no autorizado.

- El componente de Data Loss Prevention deberá permitir crear reglas de detección que se activen al contar el número de ocurrencias definidas.
- La herramienta o herramientas propuestas como parte del servicio deberán permitir el envío de notificaciones cuando se identifique una violación a las reglas establecidas
- Las bitácoras generadas por la herramienta o herramientas propuestas como parte del servicio deberán ser exportables a un SIEM.

5.2.4. PROTECCIÓN CONTRA FUGA DE INFORMACIÓN EN PUNTO FINAL.

Como parte del Servicio de Protección contra fuga de información, "EL LICITANTE" deberá controlar el uso y protección de los datos e información alojada en los equipos de cómputo del "INFONACOT", lo anterior por medio de la habilitación de una herramienta tecnológica que permita detectar y evitar la fuga y/o pérdida de información sensible, con el objetivo de contar con una completa visualización y prevención en distintas capas de seguridad.

El servicio deberá tener la capacidad de generar políticas a través de palabras clave o expresiones regulares con la información sensible, bloqueando su transmisión a través de diversos canales de comunicación desde un solo punto.

El servicio entregado por "EL LICITANTE" deberá enfocarse en prevenir fuga de información sensible, a través de los siguientes medios enunciativos más no limitativos:

a) Medios de almacenamiento removibles.
b) Correo Electrónico.
c) Aplicaciones de Mensajería Instantánea.
d) Transferencia de Archivos.
e) Impresión de información.

"EL LICITANTE" deberá configurar en la herramienta tecnológica propuesta las políticas base de seguridad definidas en conjunto con el "INFONACOT", para los equipos de cómputo, desarrollando los perfiles correspondientes. Dichas políticas deberán ser desplegadas a los equipos de cómputo del "INFONACOT", a través de la consola de administración de la solución, y el "EL ROVEEDOR" deberá garantizar la mejora continua de las mismas, con fundamento en su monitoreo continuo y los requerimientos del "INFONACOT", todo ello con la finalidad de brindar a dichos equipos de cómputo la debida protección.

"EL LICITANTE" deberá contar con personal especializado en la tecnología propuesta, para la atención de eventos y en su caso su remediación, fallas o requerimientos relacionados con la misma. Lo cual deberá acreditar a través de certificaciones vigentes en la administración de la herramienta.

El "INFONACOT" para servicio requiere inicialmente contar con la protección contra fuga de información en los puntos finales distribuidos en sus diferentes oficinas centrales y regionales, lo anterior ya que los procesos internos como el de generación de crédito utilizan información sensible y que no debe ser expuesta o filtrada, considerando en caso de ser necesario un crecimiento por unidades, con un máximo de crecimiento de acuerdo a lo requerido en la tabla de volumetrías de los servicios que se encuentra en la sección con el mismo nombre.

La herramienta tecnológica propuesta por "EL LICITANTE" para la habilitación del servicio podrá ser desplegada por medio de la herramienta de distribución de software con que cuenta el "INFONACOT". En los casos en los que no pueda ser realizado el despliegue a través de esta, "EL LICITANTE" deberá realizar la instalación en cada sitio en donde se encuentren las estaciones de trabajo sin que esto represente un costo adicional para el "INFONACOT".

"EL LICITANTE" deberá realizar consultoría de clasificación de información para establecer un procedimiento de etiquetado de la información considerando aquella que deba ser reservada y/o confidencial.

El Servicio de Protección contra fuga de información deberá cumplir con las siguientes características o funcionalidades:

- Todas las funciones de administración, incluyendo cambios y actualizaciones de configuración de políticas de protección de datos (DLP), deberán ser realizados a través de una consola de administración centralizada.
- Proveer una arquitectura centralizada a través de una sola consola Web que funja como gestor para la edición y administración de políticas, a través de módulos de detección que permita el monitoreo y generación de reportes.
- Deberá proporcionar visibilidad y control para datos en uso (endpoint) por medio de la instalación de agentes en los equipos de cómputo de los trabajadores del "INFONACOT".
- La solución de DLP endpoint deberá contar con la funcionalidad de Escaneo y brindar visibilidad de los archivos confidenciales que los usuarios tienen almacenados en sus computadoras portátiles y de escritorio.
- La tarea de descubrimiento de datos debe admitir opciones de escaneo diferencial y completo.
- Deberá poder integrarse con Active Directory o LDAP.
- Permitir a los usuarios anular las políticas proporcionando una justificación o cancelando la acción (en el caso de un falso positivo).
- La cobertura de eventos de endpoint que soportará la tecnología propuesta, de manera enunciativa mas no limitativa son:
    - Transferencia de archivos por red (SMTP, HTTP, IM, FTP, SFTP)
    - Email
    - HTTPS
    - Copiar y pegar
    - Imprimir
    - Dispositivos removibles como: USB, CD/DVD, etc.
    - Red compartida (Microsoft sharing)"
- Buscar datos que coincidan con palabras clave, expresiones (RegEx), reconocimiento del tipo o nombre de archivo y otras tecnologías de detección basadas en firmas.
- Buscar coincidencias exactas de archivos enteros o parciales, procedentes de fuentes estructuradas (por ejemplo, bases de datos) y fuentes no estructuradas (por ejemplo, archivos y folders) que se toman con un algoritmo de hash (fingerprint).

- Buscar datos no estructurados como código fuente, propiedad intelectual o contratos legales que pueda identificar mediante la construcción de un modelo estadístico basado en la carga de documentos de ejemplos positivos y negativos (Machine Learning).
- Proporcionar un método de detección eficaz basado en Huella Digital de los Datos (Fingerprinting) para cualquier tipo de dato (estructurado (bases de datos), No estructurado (documentos) y Binario (archivos no textuales)), identificando un match completo o parcial en documentos como expedientes del cliente, bases de datos, etc., para después aplicar los controles y políticas requeridas por el "INFONACOT".
- Definir un umbral o porcentaje mínimo requerido de coincidencia de un documento para considerar que existe una violación a la política configurada.
- La solución debe tener cifrado nativo o integrarse con herramientas de cifrado de terceros a través de X-Headers
- La solución deberá proteger la información sensible en dispositivo de endpoint.
- Podrá cifrar información sensible a través de una llave y permitirá el intercambio de información cifrada en medios removibles como USB, el endpoint podrá descifrar el archivo sin la necesidad de ingresar una contraseña.
- Deberá priorizar instantáneamente los casos desde niveles de riesgo alto a bajo con umbrales de puntaje de riesgo personalizables entregados en una pila de informes de clasificación de riesgo de incidentes.
- Proporcionar la capacidad de tomar huellas digitales a nivel de archivo para proteger la filtración de datos confidenciales.
- Proporcionar la capacidad de las bases de datos de huellas digitales y utilizar el hash de huellas digitales en las políticas de detección o filtración de datos.
- Deberá contar con un mecanismo de machine learning, el cual permita ingresar ejemplos positivos y negativos de documentos a proteger (códigos fuentes, archivos, etc.), para que el sistema pueda identificar información sensible automáticamente en base a esta información suministrada.
- El agente EndPoint de DLP debe estar en capacidad de monitorear los datos que sean accedidos a través de browsers como: Microsoft Edge (en OS Windows 10), Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, Mozilla Firefox ESR y Apple Safari.
- Las reglas podrán aplicarse a una sola infracción (reglas estándar) o a la acumulación de infracciones durante un período de tiempo (reglas acumulativas), las cuales acumulan coincidencias con el tiempo (pequeñas fugas de información) y crean incidentes cuando se alcanza un umbral.
- La solución debe tener políticas preconfiguradas para cumplimiento normativo, basadas en la región (país) y por tipo de industria. Principalmente basado en México.
- La solución debe proporcionar políticas predefinidas para identificar posibles expresiones que sean indicativas de acoso cibernético, patrones autodestructivos o descontento de los empleados
- Deberá realizar el análisis y protección en la transmisión de datos sensibles durante un periodo de tiempo para descubrir fuga de datos pequeñas cantidades de información (robo por goteo o robo hormiga).

- Contar con la capacidad para integrarse (a través de syslog o extracción de base de datos) con SIEM para fines de registro y alerta.
- Deberá proporcionar capacidad para escalar incidentes críticos a gerentes o propietarios de datos.
- Deberá admitir las exportaciones de informes de incidentes a través de CSV o PDF o HTML.
- Deberá tener informes predefinidos para ayudar en las investigaciones de probable fuga de información.
- Deberá admitir la capacidad de guardar informes personalizados.
- Deberá ser capaz de proporcionar datos forenses dentro del mismo registro de incidente.
- Deberá contar con la opción de enviar un pop-up donde el usuario pueda escribir una justificación, antes de permitir compartir la información; en caso de no proporcionar esta justificación, la información no podrá ser compartida en ese medio.

5.2.5. ACCESO SEGURO EN EL BORDE.

El Servicio de Acceso Seguro en el Borde deberá brindar protección ante accesos no autorizados, detección y disuasión de intrusos, reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permiso, el cual fortalecerá la protección de la frontera de la infraestructura tecnológica del "INFONACOT" contra las amenazas y actores provenientes del exterior, salvaguardando la integridad de los activos críticos del "INFONACOT".

El Servicio de Acceso Seguro en el Borde permitirá controlar las comunicaciones entre segmentos de red a nivel de capa de red, haciendo uso de políticas de seguridad para el establecimiento de diferentes niveles de confianza entre las redes, decidiendo si se permite o bloquea tráfico específico. Así mismo deberá tener la capacidad de establecer una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet.

"EL LICITANTE" para este servicio deberá considerar una implementación on- premise en el centro de datos, las oficinas centrales y remotas en donde defina el "INFONACOT", considerando un esquema en Alta Disponibilidad (HA) para el centro de datos y oficinas centrales.

Dado que cada uno de los sitios tiene requerimientos diferentes "EL LICITANTE" deberá considerar los siguientes tipos de firewalls que podrían ser requeridos dependiendo del sitio en que el "INFONACOT" solicite su instalación, considerando la cantidad de cada tipo establecida en la sección de volumetrías para este servicio.

Equipo NGFW Tipo A

Especificaciones técnicas:

- El desempeño del firewall deberá ser al menos de 36 Gbps,
- El desempeño para tráfico de NGFW deberá ser de al menos 9.0 Gbps.
- Soportar un desempeño para la protección contra amenazas (IPS) de al menos 9 Gbps
- Deberá soportar un desempeño para tráfico de tipo IPSec de al menos 20 Gbps.
- Deberá soportar al menos 30 millones de conexiones concurrentes

- Deberá soportar al menos 500,000 nuevas sesiones por segundo.
- Deberá contar con al menos 14 puertos de 1 GE y 4 puertos 10GE.
- Deberá soportar hasta 80000 túneles concurrentes de IPSEC para generación de redes virtuales privadas (VPN).
- Deberá soportar un desempeño de inspección de tráfico TLS de al menos 2 Gbps.

Equipo NGFW Tipo B

Especificaciones técnicas:

- El desempeño del firewall deberá ser al menos de 5 Gbps,
- El desempeño para tráfico de NGFW deberá ser de al menos 800 Mbps.
- Soportar un desempeño para la protección contra amenazas (IPS) de al menos 800 Mbps
- Deberá soportar un desempeño para tráfico de tipo IPSec de al menos 2 Gbps.
- Deberá soportar al menos 5 millones de conexiones concurrentes
- Deberá soportar al menos 70,000 nuevas sesiones por segundo.
- Deberá contar con al menos 8 puertos de 1 GE.
- Deberá soportar hasta 15000 túneles concurrentes de IPSEC para generación de redes virtuales privadas (VPN).
- Deberá soportar un desempeño de inspección de tráfico TLS de al menos 300 Mbps.

Equipo NGFW Tipo C

Especificaciones técnicas:

- El desempeño del firewall deberá ser al menos de 2 Gbps,
- El desempeño para tráfico de NGFW deberá ser de al menos 200 Mbps.
- Soportar un desempeño para la protección contra amenazas (IPS) de al menos 200 Mbps
- Deberá soportar un desempeño para tráfico de tipo IPSec de al menos 1 Gbps.
- Deberá soportar al menos 2 millones de conexiones concurrentes
- Deberá soportar al menos 30,000 nuevas sesiones por segundo.
- Deberá contar con al menos 8 puertos de 1 GE.
- Deberá soportar hasta 7,000 túneles concurrentes de IPSEC para generación de redes virtuales privadas (VPN).
- Deberá soportar un desempeño de inspección de tráfico TLS de al menos 150 Mbps.

Aspectos Generales

- El Servicio de Acceso Seguro en el Borde deberá ser habilitado por medio de herramientas tecnológicas que tengan características de protección propias que incluyan por lo menos:
  a. Capacidades para poder ser configurado en Alta Disponibilidad.
  b. Soporte a clientes móviles con ambientes operativos Windows, Mac, Android y iOS.
  c. Sistema Prevención Intrusos IPS con capacidades de descifrado.
  d. Control de uso por aplicación, usuario y URL.
  e. Inspección de tráfico encriptado como mínimo controlado por políticas.
  f. Proxies de Seguridad para mínimo SSH/SFTP, HTTP, HTTPS, TCP, UDP.
  g. Funcionalidad Anti-Bot, con detección de C&C multi-método.
  h. Protección contra Técnicas Avanzadas de Evasión (AETs) validada como mínimo por NSS Labs.
  i. Control de Aplicaciones.
  j. Anti-Virus, con esquemas de reputación y escaneo local.
  k. Detección Avanzada de Malware, funcionalidad de sandboxing Zero-Day.
- El hardware y software de la solución tecnológica ofertada deberán ser del mismo fabricante, con sistema operativo endurecido por el fabricante.
- En caso de contingencia la solución deberá de poder ser implementada en formato de software ya sea en equipos físicos certificados o virtuales, sin requerir procesadores especializados o específicos.
- El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls", "Virtual Contexts" o "Virtual Domains".
- La gestión del equipo deberá ser realizada desde un sistema de gestión centralizado.
- En el caso de crecimiento y/o contingencia la solución deberá poder ser instalada en equipos con procesadores x86 64-bit y/o en ambientes virtualizados como Vmware ESXi, Hyper-V o KVM.
- En el caso de que para el cumplimiento de los puntos anteriores se requiera hardware, software o licenciamiento extra deberá ser incluido.
- La solución tecnológica deberá ser del tipo Stateful con filtrado de paquetes stateless.
- La solución tecnológica deberá contar con funcionalidad del tipo circuit-level Firewall con soporte a agentes de protocolo TCP proxy.

Autenticación de usuarios

- Deberá contar con base de usuarios interna para autenticación.
- Deberá contar con integración a directorios LDAP.
- Deberá contar con integración a directorios de Microsoft Active Directory.
- Deberá contar con integración a directorios RADIUS/TACACS+.
- Deberá contar con integración a otros directorios vía un intermediario tipo RADIUS.
- Deberá contar con integración a herramientas de doble-factor de autenticación.

- Para control de acceso a la salida a Internet, antes de iniciar la navegación, deberá mostrar un portal de autentificación residente en el equipo de seguridad (portal cautivo).

Alta Disponibilidad

- Deberá ofrecer recuperación de conexiones (stateful failover) incluyendo las conexiones del tipo VPN.
- Deberá ofrecer funcionalidad tanto de Alta Disponibilidad, así como de balanceo de cargas, sin importar el número de nodos físicos o tamaño de appliance, en modo activo-activo.
- Deberá contar con la capacidad de realizar balanceo de servidores (server load balancing), via ICMP o vía agente del mismo fabricante.

Ruteo

- Deberá contar con ruteo estático IPv4 e IPv6, PBR (Policy-base routing), ruteo multicast estático.
- Deberá contar con protocolos IGMP proxy, RIPv2, RIPng, OSPFv2 y OSPFv3, BGP, PIM-SM / PIM-SSM.

IPv6

- Deberá contar con Dual Stack IPv4/IPv6
- Deberá contar con ICMPv6
- Deberá contar con DNSv6
- Deberá poder realizarse la configuración de interfaces con direccionamiento IPv6 en cualquiera de sus interfaces
- Deberá poder realizarse la configuración de interfaces con direccionamiento mixto IPv4 e IPv6
- Cuando el "INFONACOT" le indique al "LICITANTE" que llevará a cabo el proyecto de migración de la plataforma de direccionamiento IPv4 a IPv6 el proveedor deberá trabajar conjuntamente con el instituto.

Redirección a servidores de inspección de contenido

- Deberá poder realizar redirección con los protocolos HTTP y HTTPS.
- Deberá poder realizar redirección con el protocolo FTP.
- Deberá poder realizar redirección con el protocolo SMTP.

GeoProtección y GeoLocalización

- Deberá permitir la identificación del país de origen de una dirección IP.
- Deberá permitir el control de acceso fuente o destino en base al país o continente.
- Deberá permitir mostrar en tiempo real los países que generar más accesos.

Ipsec VPN

- Deberá contar con los siguientes protocolos como mínimo IKv1, IKEv2, y Ipsec con IPv4 e IPv6.
- Deberá contar con los siguientes métodos de cifrado como mínimo AES-128, AES-256, AES-GCM-128, AES-GCM-256, Blowfish, DES, 3DES.
- Deberá contar con los siguientes algoritmos MDA como mínimo AES-XCBC-MAC, MD5, SHA-1, SHA-2-256, SHA-2-512.
- Deberá contar con los siguientes protocolos criptográficos como mínimo DH group 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21.
- Deberá contar con los siguientes métodos de autenticación como mínimo RSA, DSS, ECDSA con certificados X.509, Pre-shared keys, Híbrido, XAUTH y EAP.
- Deberá contar con las siguientes opciones: IPCOMP, NAT-T, DPD (Dead Peer Detection), MOBIKE.
- Deberá contar con las siguientes configuraciones de VPN site-to-site:
  a. Policy-Based VPN.
  b. Route-Based VPN (GRE, IP-IP, SIT).
  c. Hub and Spoke.
  d. Full Mesh.
  e. Topologías de Malla parcial.
- Deberá contar con los siguientes modos de VPN:
  a. Load Sharing.
  b. Active/Standby.
  c. Ling Aggregation.
- Deberá contar con las siguientes configuraciones de cliente VPN:
  a. Cliente VPN para Microsoft Windows.
  b. Actualizaciones automáticas de configuración desde el gateway.
  c. Failover automático con Multi-Link (múltiples enlaces).
  d. Verificación de seguridad de cliente.
  e. Logon de Dominio.
  f. Soporte a cliente VPN nativo de iOS (solo Ipsec).

SSL VPN

- Plataformas soportadas con cliente:
  a. Android.
  b. Mac OS X.

c. Windows.

- Portal Web para acceso a servicios basados en HTTP y HTTPS a través de formas predefinidas y formas libres de URL.

Inspección Profunda

- Anti-Botnet:
  a. Detección basada en descifrado.
  b. Análisis de secuencia de longitud de mensaje"
- Deberá contar con detección dinámica de contexto basado en protocolo, aplicación y tipo de archivo
- Deberá contar con Anti-Malware Avanzado - a través de filtrado de archivos utilizado en políticas
- Deberá poder integrarse a un servicio de Sandboxing on-prem del mismo fabricante
- Deberá incluir un servicio de reputación de archivos
- Deberá incluir un motor de Antimalware para mínimo los protocolos FTP, HTTP, HTTPS, POP3, IMAP y SMTP
- Deberá contar con la funcionalidad de creación de firmas (fingerprinting) independiente del protocolo para TCP y UDP.
- Deberá contar con la funcionalidad de detección de anomalías y evasiones (AET - Técnicas Avanzadas de evasión) validadas como mínimo por NSS Labs.
- Deberá contar con normalización de tráfico multi-capa y firmas basadas en vulnerabilidades.
- Deberá ser capaz de crear firmas (fingerprinting) personalizadas.
- Deberá de utilizar como mínimo lenguaje basado en expresiones regulares para el desarrollo de las firmas.
- Deberá ser capaz de realizar inspección TLS.
- Deberá contar con la funcionalidad de inspección y descifrado de flujos HTTPS tanto cliente como servidor.
- Deberá ser capaz de realizar verificaciones de validez de certificados TLS.
- Deberá contar con listas de excepciones de certificados basados en nombres de dominio.
- Deberá ser capaz de detectar inundaciones (flood) de SYN/UDP
- Deberá ser capaz de limitar conexiones concurrentes y compresión de bitácora basada en interfaces
- Deberá contar con la capacidad de protección contra métodos de petición retardada del protocolo HTTP
- Deberá contar con la capacidad de reconocimiento de escaneos TCP/UDP/ICMP, stealth, o escaneos retardados en IPv4 o IPv6
- Deber contar con diversos métodos de bloqueo:

a. Bloqueo Directo
b. Reinicio de conexión (reset)
c. Blacklisting o cuarentena (local y distribuido)
d. Respuesta en formato HTML (response)
e. Redireccionamiento HTTP"

- Deberá tener la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
- La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
- El sistema deberá identificar, categorizar y controlar y visualizar tráfico aplicaciones de manera granular por usuario, grupos de usuarios y horarios.
- El listado de aplicaciones deberá actualizarse periódicamente y de forma automática.
- Capacidad de generar firmas para aplicaciones in house.
- El sistema deberá reportar en tiempo real cuáles de las aplicaciones soportadas están siendo usadas, que usuario o dirección IP lo está haciendo y cuánto tráfico está cursando.
- Para aplicaciones de tipo P2P debe controlarse con políticas de traffic shaping.
- La solución deberá ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.
- Protección contra botnets: Se deberán bloquear intentos de conexión a servidores de Botnets, para ello se debe contar con una lista de los servidores de Botnet más utilizado. Dicha lista debe actualizarse de forma periódica por el fabricante.
- Deberá contar con análisis de reputación de archivos de las siguientes modalidades:
  - Filtrado de archivos basado en políticas.
  - Categorías: archive, ejecutable, media file, Microsoft Office document.
  - Tipos: Flash, GIF, JPEG, MPEG, OLE, PDF, PNG, Riff, RTF, ZIP.

Monitoreo y gestión

- Deberá contar con mínimo una interfaz de control y gestión que le permita integrarse a un sistema de gestión centralizado como herramienta de monitoreo, análisis de bitácora (log) y reportes.
- Deberá contar con herramientas de captura de tráfico como son tcpdump, o capturas remotas desde el sistema de gestión centralizado.
- Deberá contar con esquemas de alta seguridad de 256-bit para la comunicación entre los motores de operación y el sistema de gestión centralizado.
- Deberá contar con alguna de las siguientes certificaciones de seguridad:

a. Common Criteria Network Devices Protection Profile with Extended Package Stateful Traffic Filter Firewall.

b. FIPS 140-2 crypto certificate.

c. CSPN - ANSSI.

d. Primer nivel de certificación de seguridad USGv6.

SD-WAN

- Todos los requerimientos de seguridad antes mencionados deberán funcionar en ambientes simples de interconexión o en ambientes de SD-WAN sin limitaciones
- Deberá contar con mínimo una interfaz de conexión que le permita integrarse a un sistema dinámico de control o VPN Broker para actualizaciones de configuraciones y creación de VPNs dinámicas
- Deberá contar con la capacidad de integrar conceptos de VPN tradicional o túneles tipo GRE al esquema de SD-WAN
- Deberá contar con la capacidad de integración con terceros vía túneles de VPN o túneles GRE.
- Deberá contar con conceptos de Alta Disponibilidad y Balanceo de Enlaces, y no deberá tener restricciones con respecto a la tecnología usadas en la misma
- Deberá contar con mínimo 2 métodos de balanceo, tipo RTT y Ratio
- Deberá contar con conceptos de QoS (Calidad de Servicio) integrados al ambiente de SD-WAN
- Deberá contar con conceptos de priorización y clasificación de tráfico integrados al ambiente de SD-WAN
- Deberá contar con la capacidad de creación de gateways tanto standalone, así como en cluster, e insertarlos en el ambiente de SD-WAN
- Deberá contar con la integración a un sistema de gestión centralizado, el cuál cuente con secciones específicas para el concepto de SD-WAN
- Cada nodo en el ambiente de SD-WAN no deberá tener limitantes en cuanto al número de endpoints (puertos físicos) que se le configuren y que sean requeridos para la integración del mismo.
- Deberá tener la capacidad de integrar nodos o endpoints localizados tanto en ambientes físicos, como aquellos que se ubiquen en ambientes virtuales.
- Deberá contar con la capacidad de realizar Link Aggregation en el caso de contar con múltiples enlaces y que esto no afecte la funcionalidad e integración a un esquema de SD-WAN.
- Deberá tener la capacidad de realizar decisiones de Alta Disponibilidad o Balanceo basado en el desempeño de los enlaces.
- Para el análisis del desempeño deberá considerar como mínimo los siguientes 3 conceptos de forma simultánea: Perdida de paquetes (loss of packets), Latencia (Latency) e Inestabilidad o fluctuación (Jitter).
- Deberá tener la capacidad de realizar ruteo de aplicaciones basado en su payload, lo cual permitirá el envió de cada aplicación de forma independiente a través de la malla de SD-WAN

Características generales del sistema de gestión

- El sistema de gestión deberá ser del tipo centralizado con el objetivo de gestionar múltiples equipos desde un solo punto, capaz de adaptarse al crecimiento de la infraestructura bajo demanda
- El sistema de gestión deberá residir en un equipo físico o virtual independiente de los equipos de operación
- El sistema de gestión deberá ser basado en software permitiendo así su uso en equipos estándar o virtuales.
- El sistema de gestión deberá poder ser instalado en appliance con SO propio de la marca en carácter blindado y/o robustecido o en equipos con procesador estándar sin necesidad de aceleradores o procesadores de tipo específico, usando sistemas operativos como Windows o Linux
- El sistema de gestión deberá de tener 2 componentes, un servidor de gestión y un servidor de bitácora los cuales podrán ser instalados en un mismo equipo o en equipos separados en el caso de ser requerido
- El componente o servidor de bitácora podrá ser instalado varias veces asociado a un servidor de gestión, permitiendo así la distribución del almacenamiento y envío de bitácoras de forma regionalizada.
- El componente de gestión deberá poder ser instalado en un esquema de alta disponibilidad, sin importar su ubicación física, permitiendo esquemas de activo-pasivo como mínimo, hasta un máximo de 4 instancias.
- El componente de bitácora deberá poder ser instalado bajo el esquema de multi-punto con el objetivo de que en caso de falla de uno de los componentes sea posible utilizar otro como sustituto, sin importar en donde se encuentre ubicado.
- Deberá contar con una herramienta de respaldo que le permita generar respaldos y que estos sean transportables entre Windows, Linux como mínimo sin importar si el sistema de gestión se encuentra implementado en formar física, o virtual.

Funcionalidades del sistema de gestión

- Deberá de acceder el sistema de gestión vía un Navegador.
- Deberá contar con un esquema de API que permita la integración de terceros y sus servicios al sistema de gestión centralizado
- Deberá contar con una arquitectura tipo REST que permita la utilización de códigos tipo XML o JSON
- Deberá tener la capacidad de aplicar cambios y tareas a múltiples elementos al mismo tiempo.
- Deberá contar con herramientas de limpieza y optimización que permitan a los administrados encontrar fácilmente elementos y reglas de poco uso

- Deberá contar con un sistema de alertas tipo workflow que permitan al administrador encaminar alertas del sistema utilizando correos electrónicos, mensajes SMS, SNMP traps y/o scripts personalizados.
- Deberá contar con la capacidad de crear alertas automáticas de umbrales para estadísticas en Dashboards
- Deberá contar con herramientas de resolución de problemas (troubleshooting) como mínimo:
  a. Herramienta de captura de tráfico.
  b. Diagnósticos.
  c. Generación de Snapshots.
  d. Monitoreo de sesiones.

Gestión de Políticas

- Deberá contar con la capacidad de gestionar contextos virtuales, cada uno con sus propias políticas y tablas de ruteo, tipo Multi-Gestión (Multi-Tenant)
- Deberá contar con formas predefinidas o templates de políticas, subpolíticas, variables dinámicas y secciones de comentario para mantener las políticas organizadas y entendibles
- Deberá contar con la capacidad de restringir acceso basado en aplicaciones de red o de cliente
- Deberá contar con la capacidad de identificar aplicaciones basado en su payload y restringir el acceso a las mismas
- Deberá contar con la capacidad de utilizar la información de la aplicación en el cliente a través de un agente que permita la obtención de metadata.
- Deberá contar con la capacidad de realizar control de cambios solicitando la autorización de un segundo administrador antes de aplicar las políticas
- Deberá contar con la capacidad de realizar control de acceso basado en objetos de dominio
- Deberá contar con la capacidad de realizar control de acceso basado en la identidad del usuario con o sin autenticación
- Deberá contar con la capacidad de realizar control de acceso basado en zonas asignadas a las interfaces físicas
- Deberá contar con la capacidad de realizar control de acceso basado en países y/o regiones geográficas (geolocalización)
- Deberá contar con la capacidad de realizar control de acceso basado en políticas de inspección de forma granular para evitar falso positivos
- Deberá contar con la capacidad de recuperar políticas y aplicarlas nuevamente
- Deberá contar con herramientas de optimización de políticas
- Deberá contar con herramientas de búsqueda de reglas y objetos dentro de las políticas
- Deberá contar con un sistema de roll-back en caso de fallas al momento de aplicar una configuración nueva.

- A través de los metadatos enviados por medio del agente, podrá utilizarse esta información como criterio para el control de acceso en las políticas del equipo de acceso seguro en el borde.
- Deberá poder detectar usando el agente la cantidad de clientes de puntos finales que están conectados y envían información, también se deberá poder ver qué usuarios están conectados.
- Deberá ser capaz de proteger al endpoint contra el robo de datos dentro y fuera de la red corporativa.
- Deberá de soportar las siguientes funcionales:
    - Prevenir de pérdida de datos (DLP) protegiendo a los puntos finales de la pérdida involuntaria de datos y el robo de datos.
    - Supervisar el punto final para determinar qué conexiones permite el equipo de acceso seguro en el borde.

Gestión de Conectividad

- Deberá contar con herramienta gráfica para la configuración de ruteo y rutas default
- Deberá contar con herramienta tipo CLI para gestión local
- Deberá contar con una herramienta gráfica para configurar reglas de antispoofing
- Deberá contar con herramientas de configuración automática de esquemas de antispoofing basados en el ruteo
- Deberá contar con herramientas para crear reglas de VPN basadas en:
    a. Políticas (policy-based)
    b. Rutas (Route-based)
    c. Túneles (GRE)
- Deberá contar con herramientas para crear reglas de VPN de acceso remoto basados en:
    a. Cliente VPN Ipsec (iOS y Windows)
    b. Cliente SSL VPN (Android, Mac y Windows)
    c. Portal SSL VPN (clientless para HTTP y HTTPS)

Reportes y Estadísticas

- La solución deberá incluir un módulo de reportes para visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real. Está deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional.
- Deberá contar con vistas gráficas o dashboards que muestren en tiempo real las estadísticas de red.
- Deberá mostrar la información del país asociado a la dirección IP, utilizando un símbolo con su bandera y estadísticas de geolocalización.
- Deberá mostrar con vistas gráficas el flujo de ataques en tiempo real.

- Deberá contar con una herramienta de generación de reportes personalizados y agendar su ejecución.
- La solución deberá generar reportes de: Utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y/o servicios con mayor consumo de recursos.
- La solución deberá generar reportes de los ataques detectados/detenidos con mayor frecuencia en la red, por fuente y/o por destino.
- La solución deberá generar un reporte de las actividades administrativas (entradas de administradores, cambios de configuración) realizadas.
- El sistema de reportes debe proveer información consolidada sobre al menos:
  - Top de eventos por origen
  - Top de eventos por destino
  - Eventos por fecha.
  - Eventos por semana.
  - Top de aplicaciones
  - Top aplicaciones vs users
  - Severidad"
- La solución deberá generar reportes en formato PDF o XML
- La solución deberá enviar el reporte vía correo electrónico.

5.3. Servicio Administrado de Protección de Aplicativos.

5.3.1. Firewall de aplicaciones web

El Servicio de Firewall de Aplicaciones Web tendrá la capacidad de filtrar los accesos y peticiones a las aplicaciones Web del "INFONACOT" basado en reglas y políticas definidas, así mismo, deberá tener la capacidad de ejecutar un monitoreo de estas actividades, generando bitácoras y la correspondiente explotación de dicha información, protegiendo además de amenazas externas, evitando la extracción, modificación, alteración y mal uso de la información contenida en las aplicaciones Web. El servicio deberá habilitar una herramienta tecnológica para soportar cualquier aplicación web, sin importar la plataforma, tamaño del sitio o lenguaje de implementación.

El servicio deberá ser implementado en la Fase I, al inicio del proyecto. Con la finalidad de efectuar una correcta configuración y puesta en marcha tanto del servicio administrado como de las herramientas habilitadoras del servicio, "EL LICITANTE" deberá considerar por lo menos las siguientes actividades.

- Realizar la configuración y puesta a punto de la herramienta habilitadora del servicio conforme al alcance establecido en el presente anexo técnico para este servicio, así como a las necesidades de operación del "INFONACOT" y de común acuerdo con "EL LICITANTE" adjudicado, "EL LICITANTE" deberá considerar para este servicio un esquema on-premise.
- Habilitar la protección de los aplicativos Web que se encuentran en las plataformas de Azure y AWS.
- Definir y entregar el proceso de escalamiento de incidencias y de comunicación de desviaciones de operación y de incidentes/amenazas potencialmente peligrosas.

- Realizar las pruebas de validación de las configuraciones de la herramienta habilitadora para liberar el servicio a producción.

"EL LICITANTE" deberá contar con personal especializado en la tecnología propuesta, para la atención de eventos y en su caso su remediación, fallas o requerimientos relacionados con la misma. Lo cual deberá demostrar mediante presentación de certificaciones vigentes en la administración de la solución propuesta.

El Servicio de Firewall de Aplicaciones Web deberá tener la capacidad de proteger las aplicaciones expuestas en internet del "INFONACOT" que sean acordadas con el administrador del contrato, con base en la volumetría establecida para este servicio en la sección "volumetría de los servicios".

Como parte del Servicio de Firewall de Aplicaciones Web y APIs "EL LICITANTE" deberá tener la capacidad de proporcionar las siguientes características y/o funcionalidades:

- Brindar protección contra amenazas y ataques de nivel aplicativo para las aplicaciones institucionales que tenga la capacidad de operar mediante la instalación de hardware y/o software, y deberá soportar cualquier aplicación web, sin importar la plataforma, tamaño del sitio o lenguaje de implementación.
- Tener la capacidad de inspección sin importar el tamaño, duración o tipo de ataque, enviando 100 Mbps de tráfico esperado a las aplicaciones institucionales.
- Tener la capacidad de inspección de más de 30 aplicaciones y servicios web sin importar si estas se encuentran en el Centro de Datos propio, terceros o incluso en servicios de nube pública.
- El servicio deberá cubrir todas las vulnerabilidades expresadas en el OWASP Top Ten más reciente.
- Deberá brindar soporte para tráfico SSL/TLS.
- Deberá brindar protección completa del API OWASP Top 10.
- Deberá contar con un servicio automatizado y libre de mantenimiento basado en un modelo de seguridad positiva que detecte vulnerabilidades.
- Deberá brindar eliminación del mal uso de las API.
- El servicio deberá ser capaz de realizar clasificación de clientes, basado en análisis de comportamiento, firma y huella de dispositivo.
- Deberá brindar contención por límite de peticiones (Rate Limiting).

  Deberá ser capaz de ofrecer multi-factor de autenticación para acceder al portal Web de la solución.
- Deberá ser capaz de interceptar respuestas de servidores que puedan representar un riesgo y modificarlas antes de que lleguen al cliente.
- Deberá ofrecer protección contra ataques de negación de servicio distribuido (DDoS, por sus siglas en inglés) para aplicaciones Web que esté activo todo el tiempo.
- La solución deberá tener la capacidad de ofrecer protección contra denegación de servicio desde una red red global de POPs (puntos de presencia) dedicada para la mitigación de ataques DDoS.
- Deberá soportar una red de entrega de contenido (CDN, por sus siglas en inglés) que permita al menos,
  - Aceleración de contenido dinámico.

- Compresión de archivos y recorte de código a lo más esencial para una rápida entrega.
- Optimización de la sesión.
- Optimización inteligente (Caching), basado en el perfilamiento del contenido.
- Creación de reglas personalizadas.
- Protección contra peticiones redundantes.
- Creación de Reglas para la entrega de aplicaciones.
- Deberá con la funcionalidad de balanceo de cargas global,
- Envío de bitácoras (Logs) a SIEM ya sea por SFTP, API o integración nativa.
- Habilidad de administrar la solución a través de REST API, así como para el acceso a las bitácoras (Logs) de seguridad.
- Servicio de reputación que utilice la inteligencia propia o colaborativa y de terceros.

- El servicio de identificación de amenazas debe contar con algoritmos de Big Data para agrupar múltiples eventos de seguridad según patrones recurrentes, con el objetivo de minimizar la "fatiga de alertas".
- Deberá ser capaz de almacenar 90 días la evidencia de tráfico
- Deberá permitir la creación de reportes avanzados que permita la identificación de:
  - Fortalezas.
  - Debilidades.
  - Niveles de riesgo.
  - Mejoras de implementación.
  - Monitoreo proactivo que utilice análisis estadístico para identificar comportamiento anormal o cambios que impacten en la postura de seguridad.
  - Capacidad de contención de 6 Tbps o superior.
  - Contar con un Centro de depuración DDoS.
  - Contar con un SLA del 99.999%.

5.3.2. FIREWALL DE BASE DE DATOS

El Servicio de Firewall de Bases de Datos consistirá en definir y ejecutar todas las actividades necesarias para ejercer el control y prevenir intrusiones a las Bases de Datos protegiéndolas en contra de ataques o amenazas, mediante la administración de reglas y políticas que se deberán configurar en los equipos DBF propuestos, que permita mantener un nivel adecuado de seguridad en las Base de Datos del "INFONACOT".

El Servicio de Firewall de Bases de Datos permitirá analizar el tráfico que fluye por y hacia las Bases de Datos, con el fin de tomar acciones preventivas en caso de identificar amenazas potenciales generadoras de riesgo, que pudieran ocasionar eventos de seguridad durante el proceso. Permitirá ejecutar las acciones necesarias en caso de detectar un posible ataque en progreso, protegiendo de esta manera la información confidencial almacenada en las bases de datos en contra las amenazas internas y/o ataques externos, alertando y/o bloqueando los ataques y las solicitudes anormales de acceso; brindando visibilidad del uso de la información, generando parches virtuales de las vulnerabilidades detectadas en las bases de datos. Así mismo, evitará que usuarios o atacantes hagan uso ilegítimo de los recursos tecnológicos de red que el "INFONACOT" pone a disposición de usuarios válidos.

"EL LICITANTE" deberá contar con personal especializado en la tecnología propuesta, para la atención de eventos y en su caso su remediación, fallas o requerimientos relacionados con la misma. Lo cual deberá demostrar mediante presentación de certificaciones vigentes en la administración de la solución propuesta.

En el caso de que requiera de algún agente para la protección de las bases de datos, "EL LICITANTE" deberá instalarlos y habilitarlos para la protección local de las instancias de bases de datos.

El agente deberá proporcionar el monitoreo de integridad de los archivos críticos del servidor, este agente deberá ser instalado en los activos críticos que se definan en conjunto entre "EL LICITANTE" y el "INFONACOT".

El servicio deberá ser implementado en la Fase I, al inicio del proyecto. Con la finalidad de efectuar una correcta configuración y puesta en marcha tanto del servicio administrado como de las herramientas habilitadoras del servicio, "EL LICITANTE" deberá considerar por lo menos las siguientes actividades.

- Realizar la instalación, configuración y puesta a punto de la herramienta habilitadora del servicio conforme al alcance establecido en el presente anexo técnico para este servicio, así como a las necesidades de operación del "INFONACOT" y de común acuerdo con "EL LICITANTE" adjudicado, considerando un esquema On-premise en el Centro de Datos Principal.
- Definir y entregar el proceso de escalamiento de incidencias y de comunicación de desviaciones de operación y de incidentes/amenazas potencialmente peligrosas.
- Realizar las pruebas de validación de las configuraciones de la herramienta habilitadora para liberar el servicio a producción.

"EL LICITANTE" deberá considerar para este servicio una implementación on-premise.

La herramienta o herramientas tecnológicas propuestas para proporcionar el servicio de firewall para bases de datos deberá contar como mínimo con las siguientes funcionalidades:

- Será 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.
- Brindar la protección a los servidores de bases de datos que el "INFONACOT" tiene en su centro de datos, así como a los servidores y/o servicios de bases de datos que el "INFONACOT" tiene habilitados en plataformas de nube, ya sean como IaaS o cómo SaaS.
- Realizar una evaluación exhaustiva de los riesgos de la infraestructura objetivo a diferentes niveles/capas de la infraestructura de base de datos incluyendo:
    - Aspectos de configuración de la base de datos tales como nivel de parcheo, configuración de las cuentas de usuario, evaluación de la fortaleza de las contraseñas, vigencia de contraseñas.
    - Aspectos de configuración de la plataforma, incluyendo configuración del sistema operativo de los servidores que soportan el software de base de datos.
- 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.
- Tener la capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo con las políticas de negocio. Las definiciones de tipo de dato deberán poder crearse de manera flexible y granular.
- 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.
- Apoyar en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y control de cambios.

- Monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
- Monitorear e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicativos, acceso directo a la base de datos, ligas, stored procedures, entre otros.
- Hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.
- Tener capacidad de monitorear el tráfico cifrado hacia las Bases de Datos.
- Contar con tecnología de autoaprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo esquemas, objetos, tablas, sistemas, aplicativos, campos, directorios, así como el comportamiento de cada usuario; todo esto para el establecimiento de un comportamiento base de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.
- Proporcionar protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.
- Generar reportes y tendencias en tiempo real, así como permitir la modificación de estos.
- Contar con facilidades o herramientas analíticas para la conducción de Análisis Forense cuando sea reportado algún incidente.
- La herramienta o herramientas tecnológicas propuestas para proporcionar el servicio no deberá requerir el instalar agentes de software en los servidores a monitorear, pero deberá tener la opción en caso de ser necesario.
- Funcionar independiente a la activación de la auditoría nativa de la base de datos.
- Deberá ser transparente para la base de datos y/o los aplicativos 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.
- El repositorio para el registro de la actividad de auditoría no deberá ser accesible por ningún otro mecanismo que no sea la interacción mediante la GUI (interfaz gráfica) proporcionada por el fabricante o por medios administrativos debidamente asegurados.
- Proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.
- Manejar reglas y políticas tan amplias o granulares como se requieran, deberán poder ser construidas automática o manualmente y deberán poder ser actualizadas, igualmente, de forma manual o automática.
- Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:
    - Número de registros a regresar por la consulta (SQL Query)
    - Número de registros afectados

- Tipo de datos accedido (financiero, recursos humanos, inventarios, o cualquier definición personalizada)
- Acceso a datos marcados como sensibles
- Base de Datos, Esquema, Tabla y Columna accedida
- 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 base de datos
- Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier personalización por expresiones regulares)
- Autenticación (login, logout) y tareas (quering)
- Direcciones IP 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 de las tareas
- Errores en el manejador de SQL
- Número de ocurrencias en intervalos de tiempo definidos
- Por operaciones básicas (Select, Insert, Update o Delete)
- Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate o Export)
- Por Stored Procedure o función utilizada
- Si existe evento asignado de cambios (ticket)
- Fecha y hora del evento

- Identificar individualmente a los usuarios finales que realicen actividades mediante aplicativos, aún si utilizan mecanismos comunes de comunicación entre la aplicación y la base de datos, esta actividad no deberá implicar la modificación de la aplicación y/o de la base de datos.
- Deberá posibilitar los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.
- Asociar y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son indicativos de una potencial violación de seguridad.
- Proteger contra ataques SQL y no-SQL (como buffer overflow)
- Correlacionar la actividad en las bases de datos con actividad de aplicativos web para entender detalladamente como los usuarios están accediendo datos privilegiados sin necesidad de alterar la aplicación web.
- Manejar una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.
- Tener facilidades de archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS o SCP)

- Contar con políticas, reportes, alertas, objetos sensibles, y transacciones pre-identificadas y preconfiguradas para trabajar con las siguientes plataformas empresariales: Oracle EBS, Peoplesoft, SAP.
- Tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP o Syslog.
- Analizar los eventos generados desde diferentes bases de datos. El análisis deberá contemplar los siguientes criterios:
    - Mostrar el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos.
    - Contar con un sistema de correlación basado en la dirección de los ataques. Deberá determinar si los ataques provienen desde dentro del "INFONACOT" hacia afuera de la misma o viceversa.
    - Realizar una correlación automática y en tiempo real de eventos, vulnerabilidades y bases de datos.
    - Ejecutar una correlación que permita identificar usuarios de aplicación asociados con consultas en bases de datos específicas sin necesidad de alterar aplicativos o instalar APIs.
    - Correlacionar eventos como número de errores inusuales de sentencias de SQL o al momento de hacer autenticación a las bases de datos.
- Permitir el manejo de alarmas y notificaciones –en tiempo real– para los eventos de correlación mencionados anteriormente.
- Contar con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de estas.
- Soportar la instalación en modo de clúster, además en caso de que requiera el despliegue de agentes de monitoreo de Bases de Datos, los agentes deberán poder estar asignados a un dispositivo y podrán moverse automática o manualmente según sea el caso sin necesidad de volver a registrar el agente con el dispositivo o realizar alguna acción en el servidor en el cual se encuentra instalado el agente, permitiendo enfocarse en el rendimiento de la solución como un todo.
- Ser capaz de monitorear al menos las siguientes plataformas de bases de datos:
    - Oracle
    - Microsoft SQL Server
    - MySQL
- Proporcionar un proceso de instalación, actualización y gestión de cambios centralizada, segura y ágil para los agentes; la cual deberá proporcionar una visión completa de todas las actualizaciones disponibles para los componentes de la solución de protección de bases de datos.
- Notificar cuando se encuentre disponible una nueva versión del agente de monitoreo.
- El despliegue y la instalación centralizada de parches y actualizaciones a componentes solo deberá ser realizada por usuarios con los privilegios necesarios y administradores de la herramienta.

- Proporcionar información del tráfico enviado de los agentes a los dispositivos, identificando actividades de bases de datos que no son necesarias monitorear; permitiendo a los administradores de la solución generar reglas de exclusión para reducir el consumo de recursos en el servidor.
- Contar con la opción de reducir el tráfico entre la comunicación entre el agente y el dispositivo utilizando métodos de comprensión de datos.
- Proporcionar la opción de enmascarar la información personal que se despliega a través de la interfaz de administración, además deberá contar con la opción de desenmascarar esta información dependiendo los privilegios de cada usuario.
- Deberá tener la capacidad de proteger las bases de datos en un despliegue on-premise, de nube privada o nube pública según le convenga al "INFONACOT".
- Monitorear datos y usuarios, identificar de manera inteligente, priorizar los riesgos y presentar una imagen clara y procesable de los riesgos descubiertos y detenidos.
- Contar con aprendizaje automático y análisis de grupos de personas para establecer una línea de base contextual completa del acceso típico de los usuarios a las tablas de la base de datos, detectar y prioriza la actividad anómala.
- Aprender dinámicamente los patrones de acceso a datos normales de los usuarios y luego identificar actividades de acceso inapropiadas o abusivas para alertar proactivamente a los equipos de TI sobre conductas peligrosas.
- Contar el aprendizaje para automatizar el procesamiento de grandes cantidades de registros de actividad de las bases de datos para resolver incidentes significativos.
- Contar con los algoritmos preconfigurados desarrollados para detectar el acceso a datos abusivos o inapropiados específicos, como el abuso de la cuenta de servicio o el acceso excesivo a los registros de la base de datos.
- Contar con un tablero intuitivo que proporcione un resumen ejecutivo de los riesgos de violación de datos en sus bases de datos y archivos compartidos.
- Provista con el licenciamiento o suscripciones necesarias para soportar las funcionalidades sin la necesidad de adquirir software con algún costo adicional.

Identificación de riesgos en el uso de datos

- Deberá ser capaz de:
    - Analizar el comportamiento de acceso a datos de usuarios con una vista consolidada de su base de datos.
    - Examinar los incidentes y las anomalías específicas del individuo, con base en la línea de base de la actividad típica del usuario y comparar un usuario determinado con el grupo al que pertenece.
    - Identificar incidentes de alto riesgo y priorizar lo que más importa, combinando el aprendizaje automático con las capacidades de agrupación y calificación.
    - Investigar los eventos filtrando los incidentes abiertos por gravedad, con diversos niveles detalles específicos del incidente sobre el usuario y los datos accedidos.

- Proporcionar un análisis de riesgo que permita tener una visibilidad granular de cómo los datos están siendo utilizados por quién y proporciona información para que pueda contener rápidamente un acceso no autorizado/permitido.

Monitoreo de usuarios.

- Deberá estar encargada de la identificación de que usuarios tienen derechos sobre los objetos de bases de datos, dar seguimiento al uso de esos privilegios que permitan tener el control
- Poder realizar escaneos sobre los activos de base de datos para detectar permisos sobre las diversas cuentas de usuario y recopilar información sobre quién entregó y/o recibió dichos permisos.
- Poder mostrar la organización de los permisos y usuarios para determinar si son o no, apropiados, aprobar o rechazar la asignación/recepción de los permisos o asignarlos a un supervisor.
- Para lograrlo, deberá ser capaz de identificar al menos los siguientes elementos:
  - Roles
  - Grupos de seguridad
  - Objetos
  - Cuentas
  - Privilegios
  - Permisos efectivos
  - Rutas de poder (conjunto de roles, permisos y objetos)

Plataforma

- En caso de que se requiera desplegar la solución en ambiente físico o virtual dentro de la infraestructura del "INFONACOT" (on-premise) la solución deberá ser capaz de:
  - Los diferentes componentes de seguridad de los aplicativos distribuidos en red deberán de administrarse a través de una consola centralizada.
  - Si la solución propuesta incluye equipamiento físico deberá poder ser desplegada o implementada en línea como un puente o bridge transparente (capa 2 del Modelo OSI) las interfaces no deberán requerir de una dirección IP, o como un analizador no en línea a través de puertos Mirror o SPAN.
  - Los appliances físicos deberán soportar interfaces bypass/fail-open/fail-closed configurable tanto para fallas de hardware como software.
  - En el modo monitoreo el administrador podrá visualizar alertas, ataques, errores de servidor y otra actividad no autorizada.
  - En el modo de cumplimiento de políticas, deberá bloquear ataques proactivamente.
  - Respecto de algún ataque o alguna otra actividad no autorizada, deberá ser capaz de tomar las acciones adecuadas.

- Las acciones deberán incluir la habilidad para terminar las solicitudes y respuestas, bloquear la sesión TCP, bloquear el usuario de la aplicación, o bloquear la dirección IP.
- Respecto de ataques particularmente destructivos, deberá ser capaz de bloquear la dirección IP por un periodo de tiempo configurable.
- En modo analizador de paquetes, deberá ser capaz de enviar un paquete TCP-RST a ambos extremos de la conexión. Alternativamente, si así se configura, deberá poder reportar el comportamiento anómalo, pero no tomar acción alguna.
- Deberá poder ser desplegada dentro de ambientes virtuales VMWare y/o Microsoft Hyper-V como dispositivo virtual.
- En caso de que la solución sea propuesta en appliances físicos soportará al menos 10,000 transacciones por segundo (TPS), para no impactar el desempeño de las bases de datos del "INFONACOT".
- Para los dispositivos físicos dedicados propuestos deberá contar con opciones de conectividad física como 1Gb Ethernet en UTP o Fibra Óptica tipo SX, o conectividad 10Gb en modos SR.
- Para los dispositivos físicos las interfaces de conectividad a la red deberán de ser modulares para tener la posibilidad de hacer cambios de medio como por ejemplo Cobre UTP a Fibra Óptica y viceversa, sin necesidad de cambiar el dispositivo.
- Los appliances físicos deberán tener al menos 8 interfaces 10/100/1000 GE.

- Para el despliegue de dispositivos virtuales, deberá ser capaz de:
  - Soportar despliegue en ambientes basados en VMWare ESXi.
  - Soportar el despliegue de dispositivos de protección, así como de la consola de administración centralizada de manera ilimitada.
  - En caso de que el "INFONACOT" requiera un dispositivo físico adicional, el esquema de licenciamiento deberá permitir el uso de dichas licencias y/o suscripciones que permitan obtener el máximo aprovechamiento de las características de la solución.
- El licenciamiento deberá permitir tener un despliegue de dispositivos en ambientes basados en nube privada, nube publica, físicos, o mixto sin generar costos adicionales.
- Permitir actualizaciones de productos y/o características cubiertas con la menor cantidad de licencias, las cuales podrán ser renovadas, canceladas o incrementadas anualmente.
- Ser capaz de correlacionar y discriminar de entre los eventos de seguridad para presentar en un solo panel las amenazas reales.
- Emplear mecanismos como la inteligencia artificial y aprendizaje automático que permitirá al "INFONACOT" identificar, mitigar y responder a las amenazas reales de forma rápida y decisiva.
- Los eventos de seguridad se deberán clasificar y agrupar de acuerdo con un nivel de gravedad asociado para una investigación rápida.

5.4. SERVICIO ADMINISTRADO DE SEGURIDAD BAJO DEMANDA.

Este Servicio debe considerar lo que establecen las Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento (CNBV/CUOEF) en los siguientes apartados:

- Capítulo IV Administración de riesgos, Sección Primera, Del objeto, Artículo 59, inciso b).
- TÍTULO SEGUNDO, Sección Cuarta, Apartado B, Artículo 79 inciso b) y Fracción II.

5.4.1. ANÁLISIS DE CÓDIGO ESTÁTICO Y DINÁMICO

Los análisis de código estático y dinámico se deberán realizar por medio de una plataforma que cuente con las siguientes características:

- Deberá proveerse como un servicio SaaS (Software as a Service)
- Deberá contar con un portal web por medio del cual se pueda dar seguimiento a los análisis.
- Deberá llevar el histórico de análisis realizados.
- Se podrá elegir entre diferentes tipos de políticas para realizar el escaneo estático.
- Deberá permitir crear nuevas políticas con reglas personalizadas donde al menos se debe considerar:
    - Puntuación mínima de escaneo
    - Hallazgos con CWE (Common Weakness Enumeration)
    - Hallazgos en categorías CWE
    - Hallazgos por severidad
    - Los resultados del escaneo deberán contar con al menos las siguientes secciones:
        - Resumen ejecutivo
        - Control de políticas
        - Hallazgos y recomendaciones
        - Fallas mitigadas
        - Fallas mitigadas pospuestas
    - Deberá poder definir un tiempo de resolución para las fallas encontradas
- Los resultados deberán indicar si dentro del análisis del código se identificó buenas prácticas para mitigar posibles fallas.
- Deberá tener la capacidad de analizar código de terceros
- Deberá contar con un módulo que permita identificar las vulnerabilidades y el esfuerzo para remediarlas, considerando al menos los siguientes vectores:
    - Difíciles de subsanar
    - Fáciles de subsanar
    - Vulnerabilidades de alto riesgo alto
    - Vulnerabilidades de bajo riesgo
- Deberá indicar la línea de código donde se encuentra la vulnerabilidad
- Deberá contar con un módulo para dar seguimiento a la mitigación de las fallas, indicando el estatus de las vulnerabilidades y el estatus de las mitigaciones
- Deberá permitir obtener un reporte de las vulnerabilidades encontradas, donde al menos los tipos de reporte que debe proveer son:
    - Reporte personalizable en PDF
    - Reporte detallado en PDF
    - Reporte detallado en XML
    - Reporte resumen en PDF
    - Reporte de cumplimiento PCI en PDF

- Deberá permitir configurar diferentes tipos de tableros de control (dashboards) para identificar:
  - Cumplimiento de políticas
  - Estadísticas de escaneos
  - Tiempos de escaneos
  - Histórico del estatus de hallazgos
  - Detalles de hallazgos
  - Detalles de resoluciones y mitigaciones
  - Hallazgos de vulnerabilidades de componentes de terceros

5.4.2. Protección del Servicio de Verificación de la Credencial para Votar.

El Servicio de Verificación de Datos de la Credencial para Votar permite realizar la validación de identidad de los trabajadores que pretendan tramitar un crédito, la cual le permita evitar la usurpación de identidad por medio de una verificación ante el Instituto Nacional Electoral (INE) de los datos contenidos en la credencial para votar y de las minucias de huellas dactilares de los ciudadanos.

El "LICITANTE" que resulte adjudicado deberá considerar los equipos solicitados por el INE para conectarse al servicio de validaciones de credencial para votar (SVCV). A partir de las condiciones establecidas en el convenio vigente entre el Instituto FONACOT y el INE, el licitante deberá contemplar, al menos, lo siguiente:

1. El servicio de verificación deberá garantizar la compatibilidad del algoritmo de biometría con el utilizado por el centro de datos del INE, asegurando la correcta validación de las huellas dactilares y demás parámetros biométricos conforme a las especificaciones técnicas emitidas por dicho Instituto.

2. El licitante deberá proveer dos equipos HSM (Hardware Security Module) en configuración de Alta Disponibilidad (HA), que cumplan con el estándar FIPS 140-2 Nivel 3 para el resguardo y operación de las llaves criptográficas privadas y públicas del INE.

   Dichos equipos deberán ser de propósito particular y uso exclusivo para el servicio de verificación de la credencial para votar, sin coexistencia o segmentación compartida con otros clientes, garantizando la confidencialidad e integridad de las transacciones criptográficas.

3. El licitante deberá proporcionar dos dispositivos Firewall de propósito particular y dedicados para establecer la conexión segura entre el servicio de validación de identidad y el Centro de Datos del INE. Estos deberán contar con políticas específicas de filtrado, registro de tráfico y mecanismos de trazabilidad que aseguren la protección, disponibilidad y confidencialidad de la información intercambiada.

5.5. Servicio de Gestión de Seguridad de la Información.

El "LICITANTE" deberá realizar la mejora continua de la Política General de Seguridad de la Información, políticas, procedimientos, normas, estructuras organizacionales, estándares de seguridad y funciones necesarias para el cumplimiento de los objetivos específicos de Seguridad de la Información de la Institución conforme a la estrategia del "INFONACOT", con la finalidad de asegurar que las políticas y

procedimientos estén preparados para afrontar los retos de ciberseguridad más recientes a nivel mundial.

El "LICITANTE" deberá dar cumplimiento a los requerimientos regulatorios y estándares vigentes en apego al 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, publicado el 06 de septiembre del 2021 y todas aquellas actualizaciones que se publiquen del mismo en el DOF en el periodo de la vigencia de este servicio, y considerando de manera enunciativa más no limitativa lo siguiente:

- 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.
- Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos basados en el Framework de ciberseguridad (CSF) NIST.

El LICITANTE realizará el análisis de riesgos cibernéticos, de la madurez y efectividad de los controles de seguridad de la información tanto de áreas internas del Instituto FONACOT, como de sus proveedores, así como por el cumplimiento de los objetivos generales, la Política General de Seguridad de la Información, políticas, procedimientos, normas, estructuras organizacionales, estándares de seguridad y funciones necesarias. Para ello se debe tener en cuenta lo siguiente:

El licitante ganador deberá identificar los activos que es necesario proteger, donde se define como activo a la información, documentos, software, equipos de tecnología y servicios.

- Analizar los riesgos a los que están expuestos los activos identificados:
- Identificar amenazas.
- Identificar vulnerabilidad de los activos.
- Seleccionar controles y objetivos de control.
- Determinar riesgos en base a un análisis de impacto y probabilidad.
- Determinar acciones a seguir.

El LICITANTE brindará al Instituto FONACOT el apoyo necesario para responder a requerimientos y auditorias relacionadas con la Política General de Seguridad de la Información, políticas, procedimientos, normas, estructuras organizacionales, estándares de seguridad y funciones necesarias, realizadas por entidades reguladoras y de supervisión como la CNBV y auditores externos. Por lo que elaborará reportes y proporcionará la documentación de soporte correspondiente cuando y como el Instituto FONACOT se lo solicite.

El LICITANTE deberá alinearse a lo dispuesto en el Artículo 76, Capítulo VI, Seguridad de la Información del 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, publicado el 06 de septiembre del 2021.

El "LICITANTE" deberá apoyar al Instituto a realizar los informes que contengan el resultado de las evaluaciones efectuadas a los controles de seguridad y la descripción de las acciones de mejora implementadas en el último semestre.

De acuerdo con las necesidades del "INFONACOT", "EL LICITANTE" deberá considerar personal especializado ya sea en sitio o de manera remota, para la ejecución de las actividades relacionadas al "Servicio de Gestión de Seguridad de la Información".

"EL LICITANTE" deberá considerar las siguientes actividades como alcance del Servicio: Realizar la mejora continua del Marco de Gestión de Seguridad de la Información (MGSI) conforme a la estrategia del "INFONACOT", así como elaborar la documentación requerida y apoyar en la difusión de un MGSI actualizado, en apego a las versiones vigentes a la fecha de la publicación y todas aquellas actualizaciones que se publiquen en el DOF en el periodo de la vigencia de este servicio, y considerando de manera enunciativa más no limitativa lo siguiente:

- 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.
- Marco de Gestión de Seguridad de la Información (MGSI), formatos requeridos.
- Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos basados en el Framework de ciberseguridad (CSF) NIST.

Las fases a considerar como parte de la prestación del servicio son las siguientes:

- Planear: análisis y contexto.
- Hacer: documentar, implementar y capacitar.
- Verificar: evaluación de desempeño del MGSI.
- Actuar: mejora del MGSI.

Los siguientes puntos deberán ser considerados como parte de la estrategia de Seguridad de la Información definida en el MGSI.

- Marco para la Gestión de Seguridad de la Información.
- Mejoras al diseño de los controles mínimos de Seguridad de la Información (estándares técnicos).
- Identificación, análisis y valoración de vulnerabilidades y amenazas basado en el enfoque de riesgos.
- Evaluar el desempeño de los controles de Seguridad de la Información implementados y realizar la mejora continua de estos.
- Mejora del programa de respuesta a incidentes, integrado con el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.

El alcance del MGSI se aplica a los procesos críticos del "INFONACOT", por lo que "EL LICITANTE" que resulte adjudicado le será entregado el BIA (Análisis de Impacto al Negocio), para su revisión y en conjunto con el "INFONACOT" se identifiquen los procesos críticos.

Para el mantenimiento del Marco de Gestión de Seguridad de la Información (MGSI), se deberán de utilizar las mejores prácticas como: la norma oficial mexicana NMX-I-27001-NYCE-2015 y/o al estándar internacional ISO/IEC 27001:2013, se deben utilizar las mejores prácticas, estándares y normatividad aplicable que se defina en el transcurso de la vida del contrato.

"EL LICITANTE" debe considerar planificar y ejecutar semestralmente, un análisis y la evaluación de riesgos tecnológicos sobre los activos dentro del alcance, que permita obtener una priorización basada en niveles de impacto por confidencialidad, integridad y disponibilidad, vulnerabilidad y amenaza que tenga una afectación sobre los activos que soporta los procesos críticos del "INFONACOT". deberá de utilizar alguna

de las siguientes metodologías enunciativas más no limitativas: ISO 27005, ISO 31000, OCTAVE o MAGERIT.

"EL LICITANTE" deberá considerar realizar una propuesta de madurez mediante la cual se pueda realizar la actualización y mejora de los procedimientos, formatos y planes que actualmente ya existen en el "INFONACOT".

5.6. VOLUMETRÍA DE LOS SERVICIOS.

Con la finalidad de que se realice un dimensionamiento lo más acorde a las necesidades del "INFONACOT", "EL LICITANTE" deberá tener en consideración la información de volumetrías para cada uno de los servicios que se describe a continuación:

SERVICIOS	LINEA BASE			
	UNIDAD DE MEDIDA	CANTIDAD MÍNIMA Mensual	CANTIDAD MÁXIMA Mensual	UNIDAD DE CRECIMIENTO
Servicio Administrado de SOC				
Correlación y Gestión de eventos	EPS	1500	2500	500
Ciberinteligencia	Dominios	1	2	1
	Cuentas y/o usuarios expuestos	1	10	1
Servicio Administrado de Seguridad				
Protección contra amenazas avanzadas en servidores y puntos finales	Servidor o punto final	1200	2000	1
Gestión de cuentas con acceso privilegiado	Activos	180	250	1
Filtrado de contenido web	Usuario	1200	1600	1
Protección contra fuga de información	Punto final	1200	1600	1
Acceso Seguro en el Borde				
Equipo modelo A	Equipo	1	5	1
Equipo modelo B	Equipos	0	3	1
Equipo modelo C	Equipos	0	3	1
Servicio Administrado de Protección de Aplicativos.				
Firewall de aplicaciones web	Aplicaciones Web	10	30	1
Firewall de base de datos	Base de datos	30	60	1
Servicio Administrado de Seguridad Bajo Demanda.				
Análisis de código estático y dinámico	Evento	0	2	1
Protección del Servicio de Verificación de la Credencial para Votar.	Servicio	0	1	1

5.7. MESA DE SERVICIO

"EL LICITANTE" deberá contar con una Mesa de Servicio para atender las solicitudes e incidentes que se presenten como parte de la operación del **"Servicio Administrado de Ciberseguridad"** la misma deberá integrarse con la mesa de servicio del "INFONACOT".

La Mesa de Servicio deberá permitir el registro, notificación, seguimiento para la atención a solicitudes, incidentes, problemas o requerimientos relacionados con las herramientas ofertadas como parte de su propuesta para brindar los servicios. Así como, la atención de incidentes de seguridad.

Para recibir y dar seguimiento a solicitudes de servicio e incidentes que interrumpan o degraden el servicio o atender actualizaciones, "EL LICITANTE" deberá atender las siguientes prácticas:

- Ser el único punto de contacto para reportar incidencias, contar con personal de primer nivel para proveer soporte y atención.
- Proporcionar asistencia y soporte técnico de segundo y tercer nivel, telefónico o presencial, en formato de 24x7x365, durante toda la vigencia del servicio.
- "EL LICITANTE" deberá implementar mecanismos de comunicación con el personal técnico del "INFONACOT", mediante: correo electrónico, teléfono o celular, aplicativo vía Web.
- Establecer un número telefónico para llamada local para el "INFONACOT", para el levantamiento de reportes, independientemente de proponer otras formas de reportes.
- "EL LICITANTE" deberá proporcionar asistencia técnica telefónica desde sus instalaciones, con personal capacitado y sin ningún costo adicional para el "INFONACOT".
- Proporcionar el procedimiento para el levantamiento y seguimiento de tickets. El "INFONACOT" proporcionará a "EL LICITANTE" la lista del personal autorizado para poder levantar solicitudes.
- Contar con un aplicativo para la gestión de las solicitudes y proporcionar un acceso a través de una interfaz Web a esta herramienta para el personal técnico que el "INFONACOT" designe. Toda la información relativa a cualquier solicitud deberá estar disponible a través de esta herramienta. El cual deberá estar alineado a los procesos de ITIL.
- Proporcionar el procedimiento para escalamiento de los problemas cuando estos no hayan podido resolverse en los tiempos acordados por los niveles de servicio. Dicho procedimiento deberá ser aprobado por el Administrador del Contrato que designe el "INFONACOT".
- En caso de que la falla sea atribuible a "EL LICITANTE", éste le dará una atención hasta la solución y en su caso se aplicará la deducción-penalización correspondiente de acuerdo a los niveles de servicio.
- "EL LICITANTE" deberá generar los tickets correspondientes relacionados con los incidentes y/o alertas de seguridad detectadas o identificadas por medio del monitoreo proactivo realizado desde el servicio Administrado de SOC.

- Un reporte será considerado como cerrado satisfactoriamente cuando se haya concluido exitosamente, documentado un incidente o problema presentado, regresando a la normalidad todos los conceptos o elementos involucrados, dentro de la ventana de tiempo especificada y haber aplicado la encuesta de satisfacción del usuario.

- Una vez concluida la atención y soporte de las solicitudes, el nivel de soporte correspondiente que atendió el servicio deberá notificar al responsable del servicio, vía correo electrónico y través de la herramienta de gestión de solicitudes, que se dio por concluida la atención, indicando en forma resumida la causa de la falla y la acción de solución, así como la hora en que el servicio se restablece. Este correo es necesario para cerrar el reporte.

- Será responsabilidad de "EL LICITANTE" la gestión, adquisición y mantenimiento de las herramientas y el hardware necesario con la cual opere el área de atención. Dicha área de atención fungirá como el único punto de contacto para la solución de solicitudes, incidentes, problemas y requerimientos relacionados con el servicio.

- "El LICITANTE" deberá presentar como parte integral de su propuesta técnica el procedimiento para el registro, seguimiento y atención de solicitudes, incidentes, problemas o requerimientos relacionados con las herramientas tecnológicas propuestas como como parte del "Servicio Administrado de Ciberseguridad", así como la respectiva matriz de escalamiento.

- "EL LICITANTE" deberá entregar un reporte mensual con la información de los tickets recibidos y atendidos durante dicho periodo, el cual deberá contener como mínimo la siguiente información.

    - Número de ticket.
    - Fecha y hora de creación.
    - Descripción del evento
    - Usuario que lo reportó.
    - Personal que lo atendió.
    - Fecha y hora de resolución.
    - Descripción de la solución.
    - Encuesta de satisfacción del usuario (percepción de calidad).

Se deberá entender que en cada nivel de soporte se tendrán los siguientes alcances:

Mesa de Servicio

- Genera el ticket correspondiente a la solicitud, incidente, problema o requerimiento reportado por el usuario del "INFONACOT".

- Diagnóstico inicial de la solicitud, incidente, problema o requerimiento.

- Consulta en Base de Datos de Conocimientos de "EL LICITANTE" para la resolución en caso de aplicar de la solicitud, incidente, problema o requerimiento.

- Determinar el nivel de severidad en conjunto con el "INFONACOT" y escalar en caso necesario al nivel de soporte adecuado para su atención.

Ingeniero de 2° Nivel:

- Análisis de la solicitud, incidente, problema o requerimiento reportado conforme a la solución específica.

- Análisis de registros y en caso necesario conexión remota para la resolución de la solicitud, incidente, problema o requerimiento.

- Identificar si la solicitud, incidente, problema o requerimiento requiere disparar asistencia en sitio y/o elevar la atención a tercer nivel.

Ingeniero de 3er Nivel:

- Detección de problemas de aplicación e infraestructura.

- Resolución remota o en sitio del incidente, problema o requerimiento atribuible a la aplicación y componentes de la solución.

- Levantar la solicitud de atención ante el fabricante en caso necesario.

- En casos extraordinarios en donde "EL LICITANTE" no pueda resolver el incidente o requerimiento en el tercer nivel, será necesario que escale el caso al fabricante, quien atenderá el evento y establecerá el mecanismo de resolución que corresponda, que para casos de ese tipo puede involucrar modificaciones al servicio y/o aplicación.

- **Fabricante:**

    - Remplazo de equipo (RMA) en caso de ser necesario.

    - Desarrollo de parches para solución del incidente o requerimiento en caso de ser necesario.

5.7.1. Niveles de servicio

"EL LICITANTE" deberá asignar un nivel de servicio a todas las solicitudes, incidentes, problemas y requerimientos que se tengan dentro del periodo de vigencia del servicio, lo anterior con base en la severidad de los mismos. El personal de la Mesa de Servicio determinará en conjunto con el personal del "INFONACOT" el nivel de severidad de la solicitud, incidente, problema o requerimiento con base al impacto que presente, la afectación, atendiendo las siguientes definiciones:

SEVERIDAD	DEFINICIÓN
1: Impacto Crítico	Cuando el servicio no esté operando y esto afecte la continuidad en la operación del "INFONACOT" o se presente una caída total de la infraestructura del "INFONACOT".
2: Impacto Alto	Cuando el servicio está siendo afectado de manera importante; y se presente afectación con intermitencia en la operación del servicio del "INFONACOT", siendo posible continuar con las operaciones básicas necesarias, pero a largo plazo se afectarán negativamente.
3: Impacto Medio	Cuando el servicio este afectado, pero se pueda continuar trabajando con una pérdida menor de servicios o recursos del "INFONACOT".
4: Impacto Bajo	Cuando exista un problema, pero este no afecte la operación normal del servicio. Peticiones de funcionalidad nueva, consultas, etc.

"EL LICITANTE", deberá cumplir los tiempos de atención y respuesta de las solicitudes, incidentes, problemas y requerimientos para la entrega de los servicios objeto del presente anexo técnico, atendiendo los siguientes niveles de soporte:

Responsable	Tiempo de Atención
Mesa de Ayuda	Atención telefónica dentro de los primeros 5 minutos / Vía correo electrónico dentro de los primeros 15 minutos.

Los tiempos de resolución se miden de acuerdo a las disponibilidades establecidas en los apartados DISPONIBILIDADES DEL SERVICIO y DEDUCCIONES.

Los niveles de servicio que entregue "EL LICITANTE", atenderán a las siguientes definiciones:

Soporte de 1er. Nivel: Inicia en el momento en que el personal autorizado del "INFONACOT" levanta un ticket para la atención una solicitud, incidente, problema o requerimiento vía correo electrónico o vía telefónica a través de la Mesa de Servicio, el personal de la Mesa de Servicio por parte de "EL LICITANTE" realizará el diagnóstico inicial de la solicitud, incidente, problema o requerimiento y buscará darle solución con base a la información existente en su base de conocimientos, en caso de no poder dar solución al problema asignará el caso al ingeniero de soporte de acuerdo con el nivel de severidad identificado, el cual se encargará de elaborar un diagnóstico y dará seguimiento hasta la solución del problema.

Soporte de 2do. Nivel: Se asignará un ingeniero de segundo nivel para la solución de la solicitud, incidente, problema o requerimiento, quien deberá identificar si este está relacionado con la infraestructura tecnológica o configuración de la misma y dará seguimiento en caso de que este no se pueda resolver vía telefónica a través de la Mesa de Servicio. Si fuese necesario, podrá asistir a sitio para la solución, dependiendo del diagnóstico realizado y el nivel de severidad de la solicitud, incidente, problema o requerimiento.

Soporte de 3er. Nivel: Es realizado por ingenieros especialistas certificados por el fabricante, dedicados en específico a la solución. El personal al que se asigne el incidente, problema o requerimiento tendrá como objetivo detectar cualquier falla en la aplicación y en caso necesario, levantar un caso con el fabricante, con quién coordinará la aplicación de medidas correctivas y dará seguimiento a la problemática hasta su solución.

En caso de que la solución del incidente, problema o requerimiento necesite el remplazo de equipo (RMA) o alguna solución de desarrollo del fabricante.

5.7.2. Disponibilidad del servicio

El tiempo total por mes se considerará de acuerdo a los días naturales de cada mes, según se muestra en la tabla siguiente:

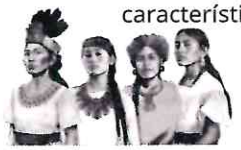
Servicio	Disponibilidad del servicio	Observaciones
Servicio Administrado de SOC	99.9%	Este servicio deberá mantener el 99.9% de disponibilidad mensual, incluyendo todas las tecnologías que forman parte del servicio
Servicio Administrado de Seguridad	99.9%	Este servicio deberá mantener el 99.9% de disponibilidad mensual, incluyendo todas las tecnologías que forman parte del servicio
Servicio Administrado de Protección a Aplicativos	99.9%	Este servicio deberá mantener el 99.9% de disponibilidad mensual, incluyendo todas las tecnologías que forman parte del servicio
Servicio Administrado de Seguridad Bajo Demanda	N/A	Al ser un servicio bajo demanda que no implica la implementación de tecnologías, no aplica para niveles de disponibilidad.
Servicio de Gestión de Seguridad de la Información	N/A	Al ser un servicio bajo demanda que no implica la implementación de tecnologías, no aplica para niveles de disponibilidad.

5.7.3. Soporte.

Todos los elementos de hardware y software del **"Servicio Administrado de Ciberseguridad"**, suministrados por "EL LICITANTE" que resulte adjudicado deberán estar cubiertos por el soporte técnico.

"EL LICITANTE" que resulte adjudicado deberá proporcionar el soporte técnico, cumpliendo en todo momento con los niveles de servicio establecidos en el presente anexo técnico.

"EL LICITANTE" que resulte adjudicado deberá proporcionar los procedimientos y formatos necesarios para el soporte técnico, además de proporcionar a su personal de soporte técnico las herramientas de hardware, accesorios, manuales, cursos de actualización y software indispensables para cumplir con las características de **"Servicio Administrado de Ciberseguridad"**.



En caso de requerir la instalación de una refacción o elemento de hardware o software de respaldo, "EL LICITANTE" que resulte adjudicado se compromete a que éstas deberán de tener características similares o superiores a las del componente afectado, cumpliendo en todo momento con los niveles de servicio requeridos.

5.7.4. MANTENIMIENTO.

Los mantenimientos a la infraestructura **Servicio Administrado de Seguridad Informática"** serán responsabilidad de "EL LICITANTE" que resulte adjudicado y no deberá generar un costo adicional para "INFONACOT". El plan de mantenimientos preventivos será definido de común acuerdo entre el "INFONACOT" y "EL LICITANTE" en las mesas de trabajo de la fase I, revisando que no afecte los períodos críticos de la operación. Los mantenimientos correctivos se ejecutarán previa notificación y autorización de "INFONACOT".

Mantenimiento preventivo

Es responsabilidad de "EL LICITANTE" que resulte adjudicado realizará el mantenimiento preventivo a los componentes tecnológicos de hardware y software proporcionados para los servicios que así lo requieran.

Las actividades a realizar durante los mantenimientos preventivos proporcionarán información relevante sobre las herramientas tecnológicas propuestas como parte del servicio, lo que permitirá:

- Evitar la degradación de los componentes de hardware por falta de limpieza, si es que la tecnología así lo requiere.
- Identificar componentes degradados o en mal estado y sustituirlos en caso de que aplique.
- Buscar posibles mensajes de error, identificar sus causas, y ejecutar las acciones necesarias para corregirlas.
- Realizar las recomendaciones sobre parches y uso de los equipos, así como la ejecución de dichas recomendaciones.

"EL LICITANTE" como parte de su propuesta deberá proporcionar el listado de las actividades consideradas para la ejecución de los mantenimientos preventivos.

Mantenimiento correctivo.

"EL LICITANTE" que resulte adjudicado efectuará el servicio de mantenimiento correctivo cuantas veces sea necesario durante la vigencia del contrato, de acuerdo con las especificaciones técnicas del fabricante.

El mantenimiento correctivo consistirá en la reparación y/o reemplazo de las partes dañadas del equipo o cuando ocurra una falla.

En los casos en los que el equipo no pueda ser reparado, "EL LICITANTE" que resulte adjudicado deberá sustituir el equipo dañado por otro de características técnicas iguales o superiores y deberá ser sin costo alguno para "INFONACOT".

6. FASES DEL PROYECTO

6.1. FASE I – IMPLEMENTACIÓN DE LAS SOLUCIONES PROPUESTAS PARA LOS SERVICIOS BÁSICOS DE SEGURIDAD.

"EL LICITANTE" que resulte adjudicado se encargará al 100% de la implementación y puesta a punto de todas las soluciones tecnológicas e infraestructura propuesta para brindar los servicios mencionados en esta fase.

"EL LICITANTE" que resulte adjudicado dotará todos los componentes necesarios (los recursos humanos, materiales, software, licencias, etc.) para el cumplimiento de los servicios en esta fase en tiempo y forma, la cual deberá quedar terminada al 100% dentro de los primeros 90 días posteriores a la notificación de adjudicación.

Sólo se pagarán los servicios que se encuentren instalados, configurados y puestos a punto y sobre servicio devengado.

"EL LICITANTE" que resulte adjudicado deberá mantener la continuidad de los servicios de seguridad informática con que cuenta actualmente el "INFONACOT", y que sean parte de la propuesta ofertada en el presente Anexo Técnico, con el fin de garantizar la continuidad operativa de los servicios de seguridad, esto desde el inicio de la vigencia del contrato y hasta que se haya realizado la instalación, migración y puesta en producción de las herramientas tecnológicas propuestas como parte de sus servicios.

A continuación, se enuncian de forma general los servicios que "EL LICITANTE" deberá implementar en esta fase como parte de los nuevos servicios tecnológicos de seguridad de la información:

- Servicio Administrado de SOC.
  - Correlación y Gestión de Eventos.
  - Ciberinteligencia.
- Servicio Administrado de Seguridad.
  - Protección contra amenazas avanzadas en servidores y puntos finales.
  - Gestión de cuentas con acceso privilegiado.
  - Protección contra fuga de información.
- Servicio Administrado de Protección de Aplicativos.
  - Firewall de aplicaciones web.
  - Firewall de base de datos.
- Servicio Administrado de Seguridad Bajo Demanda.
  - Auditoria y verificación de Respaldos.
  - Protección del Servicio de Verificación de la Credencial para Votar.
- Servicio de Gestión de Seguridad de la Información.

En esta Fase se deberá de llevar a cabo la reunión de trabajo kick off, en la cual se definirá y validará el Plan de Trabajo definitivo a detalle, que deberá incluir todas las actividades requeridas para el cumplimiento de las etapas generales del proyecto, dicha reunión será convocada y organizada de común acuerdo entre "EL LICITANTE" y el "INFONACOT".

Deberá liderar la reunión el administrador del contrato asignado por el "INFONACOT". "El LICITANTE" presentará a los actores más relevantes que conformarán el comité de administración del proyecto por parte de "EL LICITANTE", así mismo, será el responsable de realizar la gestión de las etapas del proyecto

y sus lineamientos de comunicación. El Administrador del proyecto de "EL LICITANTE" conjuntamente con el Administrador del contrato del "INFONACOT", determinarán la programación de las sesiones para las mesas de trabajo, el mecanismo de seguimiento al plan de trabajo de "EL LICITANTE" para atender todos los requerimientos que integran el desarrollo del proyecto, dicho plan deberá estar sustentando en las mejores prácticas en administración de proyectos emitidas por el Project Management Institute (PMI).

Entre otros componentes relevantes y mínimos que "EL LICITANTE" deberá entregar posteriores a dicha reunión, se encuentran:

- El Plan de Administración del Proyecto que como mínimo debe tener:
  - i. Resumen ejecutivo del entendimiento y alcance del proyecto
  - ii. Plan general de trabajo por etapas y fases del proyecto
  - iii. Estructura desglosada del trabajo

"EL LICITANTE" deberá presentar la información de manera impresa y electrónica, pudiéndose apoyar de herramientas de administración de proyectos para la presentación, por ejemplo, de diagramas de red, gráficos de Gantt, u otros que se requieran con base en las mejores prácticas.

"EL LICITANTE" que resulte adjudicado proporcionará a "INFONACOT" la evidencia de ejecución del Plan General de trabajo detallado para la implementación de los Servicios, a efecto de que "INFONACOT" los apruebe con el propósito de dar por terminada la Fase I.

"EL LICITANTE" que resulte adjudicado deberá entregar la siguiente documentación en formato electrónico e impreso diez días hábiles después de la terminación de esta fase:

- Memoria técnica de configuración de los componentes básicos de seguridad listados anteriormente y que forman parte del **"SERVICIO ADMINISTRADO DE CIBERSEGURIDAD".**
- Carta de liberación de cada uno de los servicios incluidos en esta fase.

6.2. FASE II- IMPLEMENTACIÓN DE LAS SOLUCIONES PROPUESTA PARA LOS SERVICIOS ADICIONALES DE SEGURIDAD.

"EL LICITANTE" que resulte adjudicado se encargará al 100% de la implementación y puesta a punto de las soluciones tecnológicas e infraestructura propuesta para brindar los servicios mencionados en esta fase.

"EL LICITANTE" que resulte adjudicado dotará todos los componentes necesarios (los recursos humanos, materiales, software, licencias, etc.) para el cumplimiento de los servicios en esta fase en tiempo y forma, la cual deberá quedar terminada al 100% dentro de los primeros 90 días posteriores a la adjudicación del contrato,

En esta Fase se deberá de llevar a cabo una reunión de trabajo en la cual se validará el Plan de Trabajo para la implementación de los servicios adicionales de seguridad, dicha reunión será convocada y organizada de común acuerdo entre "EL LICITANTE" y el "INFONACOT".

Deberá liderar la reunión el administrador del contrato asignado por "EL INFONACOT". El Administrador del proyecto del "LICITANTE" deberá llevar a cabo el seguimiento al plan de trabajo de "EL LICITANTE" para

atender todos los requerimientos que integran el desarrollo del proyecto, dicho plan deberá estar sustentando en las mejores prácticas en administración de proyectos emitidas por el Project Management Institute (PMI).

Entre otros componentes relevantes y mínimos que "EL LICITANTE" deberá entregar posteriores a dicha reunión, se encuentran:

- El Plan de trabajo para la implementación de los servicios adicionales de seguridad.

"EL LICITANTE" deberá presentar la información de manera impresa y electrónica, pudiéndose apoyar de herramientas de administración de proyectos para la presentación, por ejemplo, de diagramas de red, gráficos de Gantt, u otros que se requieran con base en las mejores prácticas.

"EL LICITANTE" que resulte adjudicado proporcionará a "INFONACOT" la evidencia de ejecución del Plan de trabajo para la implementación de los Servicios, a efecto de que "INFONACOT" los apruebe con el propósito de dar por terminada la Fase II.

"EL LICITANTE" que resulte adjudicado deberá entregar la siguiente documentación en formato electrónico e impreso diez días hábiles después de la terminación de esta fase:

Memoria técnica de configuración de los servicios adicionales de seguridad que forman parte del **"SERVICIO ADMINISTRADO DE CIBERSEGURIDAD".**

6.3. FASE III- ADMINISTRACIÓN, OPERACIÓN, SOPORTE Y MANTENIMIENTO DE LOS SERVICIOS BÁSICOS DE SEGURIDAD.

Esta fase iniciará inmediatamente después de la terminación de la Fase I, donde "EL LICITANTE" que resulte adjudicado deberá estar en operación al 100% de los servicios básicos mencionados en la Fase I con sus soluciones tecnológicas ofertadas.

Las actividades que se realizarán en esta fase son:

- Atención de requerimientos como altas, bajas y cambios en las soluciones tecnológicas consideradas en la fase I.
- Monitoreo y alertamiento de posibles amenazas detectadas con las diferentes soluciones de seguridad implementadas en la fase I. Atención y Respuesta a incidentes de seguridad por medio de la solución contra amenazas avanzadas en servidores y puntos finales.
- Consultoría en la gestión de Seguridad de la Información
- Generación de reportes e indicadores de seguridad informática
- Mantenimientos preventivos y correctivos de las soluciones tecnológicas utilizadas en los servicios descritos en la fase I
- Respaldos de configuraciones de las soluciones tecnológicas utilizadas en los servicios descritos en la Fase I
- Actualizaciones de las memorias técnicas de las soluciones tecnológicas utilizadas en los servicios descritos en la Fase I

Dichas actividades mencionadas en el párrafo anterior son enunciativas mas no limitativas.

"EL LICITANTE" que resulte adjudicado debe considerar la incorporación de personal certificado para la operación, administración y el soporte técnico para la prestación de los servicios.

"EL LICITANTE" deberá asignar a un administrador del proyecto de tiempo completo, para atender los requerimientos que como parte de la prestación de los servicios solicite el "INFONACOT".

"EL LICITANTE" deberá asignar durante la vigencia del contrato una mesa especializada de servicios para atender las diferentes solicitudes, incidentes, problemas o requerimientos producto de este proyecto, con capacidades y conocimientos técnicos necesarios para atender y resolver con calidad y eficiencia los requerimientos de los servicios de soporte técnico.

"EL LICITANTE" deberá realizar un respaldo de la configuración inicial entregada en la Fase I de cada una de las herramientas propuestas habilitadoras de los servicios, así mismo, deberá realizar respaldos periódicos de estas configuraciones cada tres (3) meses como mínimo y se deberán conservar estos respaldos durante la vigencia del contrato, entregando estos a solicitud del "INFONACOT" cuando así lo requiera y al término de la vigencia del contrato y sus ampliaciones.

"EL LICITANTE" deberá realizar la actualización de las memorias técnicas por lo menos cada seis (6) meses durante la vigencia del contrato o cada que se realice un cambio en los parámetros de la infraestructura implementada.

"EL LICITANTE" que resulte adjudicado deberá generar los entregables de la Fase III descritos en la sección de Entregables del presente documento.

"EL LICITANTE" deberá entregar además de los reportes periódicos, reportes específicos y reportes bajo demanda, cuyo contenido y tiempo de entrega será definido en conjunto con el Administrador del Contrato que en su momento designe el "INFONACOT". Como parte de la operación, "EL LICITANTE" deberá de llevar a cabo y coadyuvar en caso que así lo solicite el "INFONACOT", los trabajos que sean necesarios para atender las iniciativas emitidas en el 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, publicado el 6 de septiembre de 2021 en el Diario Oficial de la Federación; por ejemplo, la que describe en su Artículo 51, que las Instituciones deberán adoptar las medidas para migrar sus servicios de telecomunicaciones hacia el protocolo IPV6; por lo cual deberá contemplar los recursos humanos y tecnológicos para dar cumplimiento a lo descrito.

"EL LICITANTE" adjudicado entregará la información o documentación relacionada con los servicios proporcionados en el presente anexo, cuando así lo solicite el Órgano Interno de Control en el "INFONACOT" o demás órganos fiscalizadores o autoridades que ejercen facultades de supervisión al "INFONACOT", con motivo de las auditorías, visitas o inspecciones practicadas, de conformidad con lo establecido en los artículos 87 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 107 de su Reglamento, 32 de la Ley del Instituto de Fondo Nacional para el Consumo de los Trabajadores y 9 de la Ley de Fiscalización y Rendición de Cuentas de la Federación"

En caso de ser requerido para el correcto cumplimiento y cobertura de los niveles de servicio, "EL LICITANTE" podrá asignar personal en sitio para la atención de eventos y en su caso su remediación, fallas o requerimientos relacionados con los servicios requeridos en el presente anexo técnico, así como tareas de seguimiento, troubleshouting o auditorias, considerando para ello al menos dos recursos, los cuales

deberán traer su equipamiento informático requerido y el "INFONACOT" asignará espacio de trabajo necesario para el desarrollo de sus funciones.

FASE IV- ADMINISTRACIÓN, OPERACIÓN, SOPORTE Y MANTENIMIENTO DE LOS SERVICIOS ADICIONALES DE SEGURIDAD.

Esta fase iniciará inmediatamente después de la terminación de la Fase II, donde "EL LICITANTE" que resulte adjudicado deberá estar en operación al 100% de los servicios adicionales mencionados en la Fase II con sus soluciones tecnológicas ofertadas.

Las actividades que se realizarán en esta fase son:

- Atención de requerimientos como altas, bajas y cambios en las soluciones tecnológicas consideradas en la fase II.
- Monitoreo y alertamiento de posibles amenazas detectadas con las diferentes soluciones de seguridad implementadas en la fase II.
- Generación de reportes e indicadores de seguridad informática
- Mantenimientos preventivos y correctivos de las soluciones tecnológicas utilizadas en los servicios descritos en la fase II
- Respaldos de configuraciones de las soluciones tecnológicas utilizadas en los servicios descritos en la fase II
- Actualizaciones de las memorias técnicas de las soluciones tecnológicas utilizadas en los servicios descritos en la fase II

Dichas actividades mencionadas en el párrafo anterior son enunciativas mas no limitativas.

"EL LICITANTE" que resulte adjudicado deberá generar los entregables de la Fase IV descritos en la sección de Entregables del presente documento.

6.4. FASE V- PLAN DE EJECUCIÓN PARA LOGRAR LA TRANSICIÓN DE LOS SERVICIOS AL VENCIMIENTO DEL CONTRATO.

Previo a la conclusión del contrato, "EL LICITANTE" que resulte adjudicado deberá realizar la transferencia del servicio de regreso a "INFONACOT", o a un tercero que "INFONACOT" designe, para ello, deberá de proporcionar la documentación, entregables y servicios descritos en la sesión de entregables para esta fase. Todas las actividades de esta fase serán coordinadas con "INFONACOT".

La documentación deberá incluir la información que se generó durante la vigencia del contrato, debidamente actualizada, tomando en consideración los eventos de administración de cambios y configuración, incidentes y problemas, además de un inventario actualizado a la fecha de entrega de todos los componentes habilitadores e infraestructura auxiliar de "INFONACOT". Adicionalmente en esta fase el "LICITANTE" entregará la base de conocimientos generada durante las fases de operación.

En el caso de terminación anticipada o de finalización de la vigencia del contrato, "EL LICITANTE" que resulte adjudicado, será responsable de iniciar el proceso de respaldo de la información, del proceso de

baja, y de realizar los movimientos de resguardo, traslado y empaquetado de los respaldos propiedad de "INFONACOT" al lugar donde indique la entidad.

El retiro será realizado en coordinación con la entrega del nuevo contrato, prestador de servicios o solución que dará continuidad a la operación de "INFONACOT", observando los acuerdos operativos de migración que de un contrato a otro sean menester, y que consideren aspectos como la configuración del servicio, contraseñas y documentación necesaria para la adecuada toma de control y administración de parte del nuevo grupo y asegurando la continuidad operativa de los servicios.

Una vez adjudicado el siguiente contrato "EL LICITANTE" actual deberá revisar el plan de trabajo propuesto por el nuevo proveedor adjudicado, contando con diez días hábiles a partir de la recepción de dicho plan para observar y/o aceptar las fechas en las que deberá entregar la información y retirar la infraestructura. Se deberá de firmar una minuta de acuerdos entre ambos proveedores.

"EL LICITANTE" que resulte adjudicado deberá realizar la transferencia al nuevo proveedor de servicios una vez concluido el contrato, contemplando un periodo máximo de 90 días a partir de la fecha de término del contrato o su extensión conforme a ley, sin que esto genere un costo o cargo para el "INFONACOT" en dicho plazo y considerando que durante este periodo no deberá haber ninguna modificación a las configuraciones de las herramientas propuesta como parte de los servicios, con excepción de las derivadas por un evento critico de seguridad.

Condiciones Técnicas para la transición a un Nuevo Prestador de servicios al término del Contrato:

La obligación de "EL LICITANTE" que resulte adjudicado durante el periodo de transición a un nuevo prestador de servicios, se deberá realizar bajo las siguientes condiciones:

a) Cumplir con los Niveles de Servicio durante el período de transición

"EL LICITANTE" que resulte adjudicado, cumplirá con los Niveles de Servicio durante el periodo de transferencia de servicios al nuevo prestador de servicios.

Durante dicho periodo, las actividades responsabilidad de "EL LICITANTE" que resulte adjudicado deberán realizarlas personal capacitado que haya estado participando en la entrega de los servicios de administración, operación, soporte y mantenimiento recurrentes (fase III y fase IV).

b) Coordinación con el nuevo prestador de servicios para realizar la migración progresiva del "nuevo proyecto"

"EL LICITANTE" que resulte adjudicado, durante el periodo de transición hacia el nuevo prestador de servicios que hubiese designado el "INFONACOT", integrará un "Grupo de Migración" y mesas de trabajo para la coordinación en esta etapa, estableciendo un plan de trabajo donde se reflejen los límites de cada uno de los participantes: Prestador del Servicio, personal de "INFONACOT", y Nuevo Prestador de Servicios, con el objeto de no afectar la operación del "INFONACOT".

"EL LICITANTE" que resulte adjudicado deberá entregar la siguiente documentación 15 días antes de la terminación del contrato:

- Memoria técnica actualizada de la configuración de todos los componentes del **"SERVICIO ADMINISTRADO DE CIBERSEGURIDAD".**
- Respaldos de las configuraciones de las herramientas que fueron habilitadas como parte de los servicios.

- Base de Conocimiento generada durante las fases de operación.

El calendario para todas las fases es el siguiente:

FASE	DESCRIPCIÓN	FECHA INICIO	FECHA FIN
FASE I	Implementación de la solución propuesta para los servicios básicos de seguridad	Primer día del inicio de la vigencia del contrato	90 días naturales después de la fecha de inicio de la fase I
FASE II	Implementación de la solución propuesta para los servicios adicionales de seguridad	Primer día del inicio de la vigencia del contrato	90 días naturales después de la fecha de inicio de la fase I
FASE III	Administración, operación, soporte y mantenimiento de los servicios adicionales	1 día natural después de la terminación de la fase I	Último día de la vigencia del contrato
FASE IV	Administración, operación, soporte y mantenimiento de los servicios adicionales	1 día natural después de la terminación de la fase II	Último día de la vigencia del contrato
FASE V	Plan de ejecución para lograr la transición de los servicios al vencimiento del contrato	1 día natural después de la terminación de la fase III y IV	90 días naturales antes de la finalización de la vigencia del contrato

7. CONDICIONES DE ENTREGA.

Condiciones generales de entrega:

Los servicios serán entregados en cualquiera de las localidades mostradas en la siguiente tabla:

Región	Nombre de Sucursal	Domicilio
Centro	Vallejo	Norte 45 No. 853-B, Col. Industrial Vallejo, Del. Gustavo A. Madero, C.P. 02300, México, Ciudad de México.
Centro	San Antonio Abad	San Antonio Abad No. 150, Col. Tránsito, Del. Cuauhtémoc, C.P. 06820, México, Ciudad de México.
Centro	Mixcoac	Molinos No. 50 Col. Mixcoac C.P. 03910 Del. Benito Juárez, Ciudad de México.
Centro	Iztacalco	Av. Añil 571 Planta Baja, Colonia Granjas México, Demarcación Territorial Iztacalco, C.P. 08400, Ciudad de México.
Centro	Tlalnepantla	Av. Sor Juana Inés de Cruz, No. 22 Despacho 106-4, Colonia Centro de Tlalnepantla, C.P. 54000, Tlalnepantla de Baz, Estado de México.
Centro	Cuautitlán Izcalli	Av. Huehuetoca s/n, SORIANA, Loc. 6, Col. Claustro de San Miguel, Cuautitlán Izcalli, Estado de México.
Centro	Chalco	Bernardo Reyes No. 1 Col. San Sebastián C.P. 56600 Chalco de Covarrubias
Centro	Ecatepec	Av. Insurgentes 102, Locales 8, 9, 10 y 11 (Grand Plaza), Colonia El Calvario, San Cristóbal Centro, C.P. 55020, Ecatepec de Morelos, Estado de México
Centro	Insurgentes	Insurgentes Sur 452, Planta Baja, Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, Ciudad de México.
Centro	Coapa	Av. Canal de Miramontes 3280, locales 27, 28, 29, 30, Coaplaza, Col. Villacoapa, Del. Tlalpan, C.P. 14390, Ciudad de Méx.
Centro	Plaza de la República	Plaza de la República No. 32, Planta Baja, Col. Tabacalera, Del. Cuauhtémoc, C.P. 06030, Ciudad de México.
Centro	SAT BANCEN	Av. Hidalgo 77, Col. Guerrero, Del. Cuauhtémoc, C.P. 06300, Ciudad de México.
Centro	Texcoco	Prolongación 16 de Septiembre No. 310, Loc. 30, Col. Barrio de San Pablo Centro, C.P 56116, Texcoco, Estado de México.
Centro	Tizayuca	Carretera México- Pachuca Km. 50, oficina de CANACINTRA Tizayuca, Zona Industrial Tizayuca, C.P. 43800, Tizayuca, Hidalgo.
Centro	Acapulco	Av. Costera Miguel Alemán No. 1803, Frac. Magallanes, C.P. 39670, Acapulco, Guerrero.
Centro	Cuernavaca	Plan de Ayala No. 501, Local 26A B y C. Col. Teopanzolco, Plaza Arcos Cristal, C.P.62350, Cuernavaca, Morelos.
Centro	Toluca	Ignacio Allende Sur No. 116, Col. Centro, C.P. 50000, Toluca, Estado de México.
Centro	Pachuca	Carr. Pachuca- Tulancingo No. 1000, Loc. D9 al D12, Plaza Universidad, Col. Abundio Martínez, C.P. 42184, Mineral de la Reforma, Hidalgo.
Centro	Cuautla	Galeana No. 33, Loc. 101, planta alta, Col. Centro, C.P. 62740, Cuautla, Morelos.

Centro	Lerma	Toluca Zona Conurbada ubicada en Av. Paseo Tollocan No. 1195, Colonia Santa María Totoltepec, C.P. 50245, Toluca, Estado de México.
Centro	Tula	Antigua Carretera México Querétaro Km 11 Col. Santiago Tlautla, Tepeji
Centro de Datos	Centro de Datos Primario del Proveedor del Servicio	Parque Industrial, Privada de la Princesa 4, 76246 Qro.
Edificio Principal	Edificio Principal	Insurgentes Sur 452, Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, Ciudad de México.
Norte	Monterrey II	Av. Ruiz Cortines y General Bonifacio Salinas 600, Col. León XIII, C.P. 67120 Guadalupe N.L. Sucursal Soriana Lindavista.
Norte	Cd. Victoria	Palacio Federal, Calle Juan B. Tijerina sin Número, entre José María Morelos y Matamoros, Zona Centro, CP. 87000 Cd. Victoria, Tamaulipas
Norte	Durango	Aquiles Serdán No. 954, planta alta, Victoria de Durango Centro, C.P. 34000, Durango, Durango.
Norte	Chihuahua	Calle Ramírez Calderón No. 901, Col. San Felipe, C.P. 31203, Chihuahua, Chihuahua.
Norte	Mexicali	Av. Reforma No. 692, Esq. Nicolás Bravo, Col. Centro 1ª Sección, C.P. 21100, Mexicali, Baja California
Norte	Hermosillo	Volved. Luis Donaldo Colosio No. 323, Col. Valle Grande, C.P. 83205, Hermosillo, Sonora.
Norte	Mazatlán	Av. Ejército Mexicano No. 1401-A, Col. Ferrocarrilera, C.P. 82010, Mazatlán, Sinaloa.
Norte	Cd. Juárez	Av. Adolfo López Mateos No. 708, locales 8 y 9 (Plaza Delta), Col. Los Nogales, C.P. 32350, Ciudad Juárez, Chihuahua.
Norte	Monterrey	Av. Melchor Ocampo No. 330 y 340 Ote, Col. Centro, C.P. 64000, Monterrey, Nuevo León.
Norte	Tampico	Av. Hidalgo No. 2401, Col. Reforma, C.P. 89140, Tampico, Tamaulipas.
Norte	Torreón	Av. Morelos No. 138 Poniente, Col. Centro, C.P. 27000, Torreón, Coahuila.
Norte	Saltillo	Blvd. Venustiano Carranza No. 3480, Col. Jardín, C.P. 25240, Saltillo, Coahuila.
Norte	Monclova	Calle Venustiano Carranza No. 410, locales 2, 3 y 4, Colonia Centro, C.P. 25700, Monclova, Coahuila.
Norte	Reynosa	Herón Ramirez Esq. con Michoacán No. 400, Locales 4, 5 y 6 Col. Rodríguez, C.P. 88630, Reynosa, Tamaulipas.
Norte	Matamoros	Av. Prolongación González No. 2035 Col. Parque Industrial, Plaza Comercial Soriana Laguneta, C.P. 87479, Matamoros, Tamaulipas.
Norte	Culiacán	Gral. José Aguilar Barraza No. 1297 Poniente, Col. Centro Sinaloa, C.P. 80000, Culiacán, Sinaloa.
Norte	Tijuana	Blvd. Díaz Ordaz No.14910, Col. Las Brisas, Plaza Las Brisas, C.P. 22115 Tijuana, Baja California.

Norte	La Paz	Calz. Forjadores de Sudcalifornia No. 286, Col. Bellavista, C.P. 23078, La Paz, Baja California Sur.
Norte	Los Mochis	Av. Cuauhtémoc No. 201 Poniente, Col. Bienestar, C.P. 81280, Los Mochis, Sinaloa.
Norte	Cd. Obregón	Durango No. 245 Sur, Col. Centro, C.P. 85000, Ciudad Obregón, Sonora.
Norte	Delicias	Circuito Plaza de la Republica 4 Norte, Colonia Centro Entre calle Central y calle 2da. Norte C.P. 33000
Norte	Empalme	Plaza Reforma, Loc.5, Col. Moderna, C.P.85330, Empalme, Sonora.
Norte	San José del Cabo	Carretera Transpeninsular Km. 34.5, Col. Guaymitas, Plaza Guaymitas, Loc. 2, C.P. 23407, San José del Cabo, Los Cabos, Baja California Sur.
Norte	Nogales	Av. de los Nogales No. 277, Loc. 3, 4 y 5, Plaza Coyoacán, Col. Colinas del Yaqui, C.P. 84093, Nogales, Sonora.
Norte	Ensenada	Av. Delante fracción A y B, Lt. 007, Mza. 025, Col. Carlos Pacheco, C.P. 22890, Municipio de Ensenada, Baja California Norte.
Norte	Gómez Palacio	Av. Hidalgo No. 113 Sur, Loc. 4, Col. Centro, Gómez Palacio, Durango.
Norte	Cd. Acuña	Libramiento Emilio Mendoza Cisneros No. 1315, centro comercial MERCO, Col. Benjamín Canales, C.P. 26236, Cd. Acuña, Coahuila.
Norte	Piedras Negras	Blvd. Eliseo Mendoza Berrueto s/n, Plaza Ciento Tres, Loc. 5, Col. San Felipe Norte, C.P. 26070, Piedras Negras, Coahuila.
Norte	Nuevo Laredo	Calle Héroe de Nacataz y Reynosa s/n, anexo al Centro Cívico, Zona Centro, CP 88000, Nuevo Laredo, Tamaulipas.
Norte	Agua Prieta	Calle 52 entre Avenida 6 y 9 Colonia Bicentenario C.P 84269, Agua Prieta, Sonora. Referencia Edificio SEDATU.
Norte	Guamúchil	Calle Francisco Villa No. 636 Sur, Col. Centro, C.P. 81400, Guamúchil, Sinaloa.
Norte	Mulege	Carretera Transpeninsular Km. 1 s/n Col. Centro, C.P. 23920, Santa Rosalía, Mulege, Baja California Sur. (Oficina Conapesca y SAGARPA)
Norte	Cabo San Lucas	Los Aguajitos s/n Col. Arcos del Sol, C.P. 23478, Cabo San Lucas, Los Cabos, Baja California Sur
Norte	Sabinas	Cuauhtémoc No. 955 poniente, Col. Federico Berrueto Ramón, C.P. 26730, Cd. Sabinas , Coahuila.
Occidente	Guadalajara II	Av. Dr. Roberto Michel No. 1003 esquina Salvador López Chávez local sub ancla 3 (Centro Comercial Parques Guadalajara) Col. Olímpica, Guadalajara, Jal.
Occidente	Manzanillo	Av. Elías Zamora Verdusco No. 2114 A, locales 1 y 2, Plaza Lauret, Barrio V, Col. Valle de las Garzas, C.P. 28219, Manzanillo, Colima.
Occidente	Puerto Vallarta	Av. Francisco Villa No. 1474, P.B., Col. Los Sauces, C.P. 48328, Pto Vallarta, Jal.

Occidente	Morelia	Av. Lázaro Cárdenas No. 2000, Col. Chapultepec Sur, C.P. 58260, Morelia.
Occidente	Guadalajara	Av. Lázaro Cárdenas No. 2305, edificio H, Loc. 102, Plaza Comercial Abastos, Col. Las Torres, C.P. 44920, Guadalajara, Jal.
Occidente	León	Juan José Torres Landa Oriente 1007, Loc. 14 y 15, Col. Puerta San Rafael, C.P. 37480, León, Guanajuato.
Occidente	Querétaro	Av. Manuel Gutiérrez Nájera No. 113, Col. Centro, C.P. 76000, Querétaro, Querétaro.
Occidente	San Luis Potosí	Mariano Arista No. 710, Zona Centro, C.P. 78000, San Luis Potosí, San Luis Potosí.
Occidente	Aguascalientes	Av. López Mateos Oriente No. 520, Col. Barrio de la Purísima C.P. 20259, Aguascalientes, Aguascalientes.
Occidente	Colima	Calle Gabriela Mistral 350, Col. Lomas de Circunvalación, C.P. 28010, Colima
Occidente	Tepic	Av. Tecnológico No. 3983, Loc. 8, 9 y 10, Col. Ciudad Industrial, Practiplaza Oriente, C.P. 63173, Tepic, Nayarit.
Occidente	Zacatecas	Blvd. José López Portillo No. 303, Planta Baja, edificio STPS, Col. Dependencias Federales, C.P. 98618, Zacatecas, Zacatecas.
Occidente	Lázaro Cárdenas	Av. Melchor Ocampo, No. 31, Locales 4 y 5 (Plaza Costa Azul), Colonia Segundo Sector de Fidelac, C.P. 60953, Lázaro Cárdenas, Michoacán.
Occidente	Celaya	Blvd. Adolfo López Mateos No. 932 Poniente, Col Centro, C.P. 38000, Celaya, Guanajuato.
Occidente	Uruapan	Av. Chiapas, No. 401 locales 6 y 7, Colonia Ramón Farías, C.P. 60050, Uruapan, Michoacán.
Occidente	Zamora	Amado Nervo Poniente No. 70, Col. Centro, C.P. 59600, Zamora, Michoacán.
Occidente	Cd. Valles	Carranza 53, Col. Centro, C.P. 79000, Ciudad Valles, San Luis Potosí.
Occidente	Fresnillo	Paseo del Mineral No. 101-B, Col. Luis Donaldo Colosio, C.P. 99036, Fresnillo, Zacatecas.
Occidente	San Juan del Río	16 Septiembre No. 8, Loc. 1, Col. Centro, C.P. 76800, San Juan del Río, Querétaro.
Occidente	Irapuato	Av. Guerrero No. 1871, Local 2, (entre Orquídea y Jazmín), Col. Gámez, C.P. 36650. Irapuato, Guanajuato.
Occidente	Matehuala	José Maria Morelos No. 427, Col. Centro, C.P. 78700, Matehuala, San Luis Potosí.
Occidente	Zapopan	Prolongación Avenida Laureles 300, Colonia Tepeyac C.P. 45150, Zapopan, Jalisco.
Sur	Xalapa	Diego Leño S/N, Col. Centro, CP 91000, Xalapa, Veracruz
Sur	Playa del Carmen	Av. Benito Juárez, Lt. 3, Loc. 12 y 13, Plaza Papagayos, Col. Centro, C.P. 77710, Playa del Carmen, Quintana Roo.

Sur	Cozumel	Plaza del Sol, Mercado de Artesanía, Local Planta Alta 8 Andador 5ta. Avenida Sur No. 1 Col. Centro C.P. 77600
Sur	Mérida	Paseo Montejo No. 492-A por la 43, Col. Centro, C.P. 97000, Mérida, Yucatán.
Sur	Tlaxcala	Av. Ocotlán No. 15, Col. Ocotlán, C.P. 90100, Tlaxcala, Tlaxcala.
Sur	Puebla	Calle 9 Norte No. 208, Col. Centro, C.P. 72000, Puebla, Puebla.
Sur	Veracruz	Av. Salvador Díaz Mirón 2870, Col Electricistas CP. 91916, Veracruz
Sur	Villahermosa	Benito Juárez No. 118-120, Col. Centro, C.P. 86000, Villahermosa, Tabasco.
Sur	Tuxtla Gutiérrez	3a Norte Poniente No. 1395, entre la 12 y 13 Poniente Norte, Col. Moctezuma, C.P. 29030, Tuxtla Gutiérrez, Chiapas.
Sur	Oaxaca	Calzada Héroes de Chapultepec No. 1104, Colonia Jalatlaco, C.P. 68080, Oaxaca. Oax.
Sur	Cancún	Av. Tulum, Retorno 1, Lote 3, Manzana 1, Súper manzana 22, Col. Centro, C.P. 77500, Benito Juárez, Quintana Roo.
Sur	Campeche	Av. 16 de Septiembre s/n, Palacio Federal, Col. Centro, C.P. 24000, Campeche, Campeche.
Sur	Tuxtepec	Av. 20 de noviembre s/n, Col. La Piragua, C.P. 68300, Tuxtepec, Oaxaca.
Sur	Coatzacoalcos	Av. Benito Juárez No. 511, Col. Centro, C.P. 96400, Coatzacoalcos, Veracruz.
Sur	Cd. del Carmen	Av. 10 de Julio No. 117 Col. Francisco y Madero CP. 24190 Cd. Del Carmen, Campeche
Sur	Córdoba	Av. 1, boulevard fundadores 2271, Col. Centro, CP 94500, Córdoba
Sur	Chetumal	Avenida Independencia No. 134, Colonia Chetumal Centro, C.P. 77000, Municipio de Othón P. Blanco
Sur	Tehuacán	Calle 1 Norte No. 618, Loc. 8, 9 y 10, Plaza Montecarlo, Col. Francisco Sarabia, C.P. 75730, Tehuacán, Puebla.
Sur	Tapachula	Av. Central Sur No. 76 Col. Centro, C.P. 30700, Tapachula Chiapas.
Sur	Poza Rica	20 de noviembre 110, Col. Cazones, CP 93230, Poza Rica de Hidalgo
Sur	Salina Cruz	Calle 5 de Mayo No. 304, Las Hormigas, C.P. 70670, Salina Cruz, Oaxaca.
Sur	CIS Puebla	Centro Integral de Servicios (CIS), Edificio SUR, Vía Atlixcayotl No. 1101.
Sur	San Cristóbal de las Casas	Calle Crescencio Rosas No. 61, Col. Barrio San Diego, Oficina Canaco, C.P. 29270, San Cristóbal, Chiapas.
Sur	Apizaco	Jesus Carranza No 213 Local 201, col. Centro C.P 90300, Apizaco, Tlaxcala

8. ENTREGABLES.

"El LICITANTE" que resulte adjudicado como parte del **"Servicio Administrado de Ciberseguridad"** deberá proporcionar al "INFONACOT" los entregables que se generen en las diferentes fases de ejecución del proyecto; los cuales deberán entregarse a periodo vencido del mes inmediato anterior, conforme al plan de trabajo establecido y a la tabla siguiente. Todos los entregables deberán ser firmados por el representante legal de "EL LICITANTE". Los formatos de los entregables serán definidos por "INFONACOT" y se validarán en conjunto con el "LICITANTE".

Entregables de la FASE I. Implementación de las Soluciones Propuestas para los Servicios Básicos de Seguridad.

Nombre del Entregable	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse
1. Minuta de Reunión de Kick off	Minuta donde se describan los acuerdos de la reunión de kick off y en donde se establecerán las mesas de trabajo, con la presentación inicial para el arranque de las operaciones del proyecto. • Este documento deberá mostrar lo que se espera del proyecto y las funciones de cada perfil participante. Permitiendo que todos tengan la misma visión de las tareas que necesitan ser realizadas para el éxito de la ejecución durante la vigencia del contrato.	Hasta 5 días hábiles posteriores a la fecha de adjudicación del contrato.	Impreso o Electrónico, en formato PDF.
2. Plan de Administración del Proyecto	Plan de Administración del proyecto que como mínimo debe tener: i. Resumen ejecutivo del entendimiento y alcance del proyecto ii. Plan general de trabajo por etapas y fases del proyecto iii. Estructura desglosada del trabajo El plan general de trabajo deberá considerar los tiempos estimados y deberá fungir como el documento a través del cual se dará seguimiento a los avances del proyecto, mismo que deberá ser aprobado por el "INFONACOT".	Hasta 5 días hábiles posteriores a la junta de inicio del proyecto (Kick off).	Impreso o Electrónico, en formato Microsoft Project 2013 o superior.
3. Reportes de avance del proyecto	"LICITANTE" deberá entregar avances y posibles desviaciones al plan general de trabajo. • Avances del proyecto • Posibles desviaciones al plan general de trabajo.	Hasta 3 días hábiles posteriores a las reuniones de avance del proyecto.	Impreso o Electrónico, formato libre
4. Calendario de Mantenimientos preventivos	"LICITANTE" deberá entregar el calendario de mantenimiento preventivos propuestos para toda la vigencia del contrato.	Hasta 7 hábiles días después del inicio del contrato	Impreso o Electrónico, formato libre

Nombre del Entregable	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse
5- Procedimientos del SOC	"LICITANTE" deberá entregar los procedimientos a utilizar para el servicio del OSC	Hasta 10 hábiles días después del inicio del contrato	Impreso o Electrónico, formato libre
6. Matriz de riesgos para la implementación del proyecto	Reporte que describa los riesgos que se pueden presentar durante la instalación, configuración, operación y/o actualización de los equipos. • Nivel de impacto • Tipo de afectación • Posible tiempo de afectación • Plan de mitigación	Mensualmente durante los primeros 7 días naturales de cada mes siguiente al mes vencido.	Impreso o Electrónico, Microsoft Word.
9. Matriz de escalamiento	Documento que contenga los datos de las personas que serán designadas para la atención y ejecución del proyecto. • Nombre. • Puesto y/o Rol. • Actividades que desempeñarán durante el proyecto. • Correo electrónico. • Número telefónico de oficina. • Extensión (cuando aplique). • Número telefónico móvil.	Hasta 5 días hábiles posteriores a la fecha de notificación del fallo	Impreso o Electrónico en formato PDF.
10. Relación del personal asignado al proyecto.	Documento con la relación del personal que estará asignado al proyecto, al cual se deberán adjuntar los CV´s y certificaciones correspondientes.	En la primera reunión inicial de las mesas de trabajo.	Impreso o Electrónico en formato PDF.
11. Memorias técnicas	Documento donde se describa la configuración, implementación, operación y comunicación de la infraestructura tecnológica que haya sido habilitada para la prestación de los servicios descritos en el presente anexo técnico. • Descripción general del servicio o dispositivo. • Inventario de dispositivos (activos) utilizados e instalados. • Capacidades del dispositivo. • Funcionalidades habilitadas en el dispositivo. • Descripción técnica de la implementación. • Diagrama Físico y lógico de la implementación. • Mapeo de puertos. • Procedimientos de respaldo.	Diez días hábiles posteriores a la fecha en que concluya la fase de implementación.	Impreso o Electrónico, Microsoft Word y PDF.

Nombre del Entregable	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse
	• Evidencias de pruebas de liberación de los Servicios, las cuales deberán ser aceptadas por el "INFONACOT".		
12. Procedimientos para la atención a través de la mesa de servicio	Documento que contenga el procedimiento a seguir para la atención para las solicitudes, incidentes, problema o requerimientos, el cual deberá ser aprobado por el "INFONACOT".	Hasta 5 días hábiles posteriores al inicio de la vigencia del contrato	Impreso o Electrónico, Microsoft Excel.
13-Acta entrega de Implementación de los servicios de la fase I	"LICITANTE" deberá entregar carta donde haga la entrega de los servicios de la fase I	Hasta 7 días hábiles de acuerdo al calendario de la terminación de la fase I	Impreso o Electrónico, Microsoft Excel.

Tabla 8. Entregables de la gestión del proyecto

Entregables de la FASE II. Implementación de las Soluciones Propuestas para los Servicios Adicionales de Seguridad.

Nombre del Entregable	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse
13. Plan de trabajo para la implementación de las soluciones adicionales de seguridad.	Plan de trabajo para la implementación de las soluciones adicionales de seguridad. • El plan de trabajo deberá considerar los tiempos estimados y deberá fungir como el documento a través del cual se dará seguimiento a los avances de la implementación de las soluciones adicionales de seguridad, mismo que deberá ser aprobado por el "INFONACOT".	Hasta 5 días hábiles posteriores a la reunión de trabajo de la implementación de la fase II	Impreso o Electrónico, en formato Microsoft Project 2013 o superior.
14. Reportes de avance de la implementación de las soluciones adicionales de seguridad	El "LICITANTE" deberá entregar avances y posibles desviaciones al plan de trabajo. • Avances de la implementación de las soluciones adicionales de seguridad. • Posibles desviaciones al plan de trabajo.	Hasta 3 días hábiles posteriores a las reuniones de avance del proyecto.	Impreso o Electrónico, formato libre

Nombre del Entregable	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse
15. Matriz de riesgos para la implementación de las soluciones adicionales de seguridad	Reporte que describa los riesgos que se pueden presentar durante la instalación, configuración, operación y/o actualización de los equipos. • Nivel de impacto • Tipo de afectación • Posible tiempo de afectación • Plan de mitigación	Mensualmente durante los primeros 7 días naturales de cada mes siguiente al mes vencido.	Impreso o Electrónico, Microsoft Word.
16. Memorias técnicas	Documento donde se describa la configuración, implementación, operación y comunicación de la infraestructura tecnológica que haya sido habilitada para la prestación de los servicios descritos en el presente anexo técnico. • Descripción general del servicio o dispositivo. • Inventario de dispositivos (activos) utilizados e instalados. • Capacidades del dispositivo. • Funcionalidades habilitadas en el dispositivo. • Descripción técnica de la implementación. • Diagrama Físico y lógico de la implementación. • Mapeo de puertos. • Procedimientos de respaldo. • Evidencias de pruebas de liberación de los Servicios, las cuales deberán ser aceptadas por el "INFONACOT".	Diez días hábiles posteriores a la fecha en que concluya la fase de implementación de las soluciones adicionales de seguridad.	Impreso o Electrónico, Microsoft Word y PDF.
17-Acta entrega de Implementación de los servicios de la fase II	"LICITANTE" deberá entregar carta donde haga la entrega de los servicios de la fase I	Hasta 7 días hábiles de acuerdo al calendario de la terminación de la fase II	Impreso o Electrónico, Microsoft Excel.

Tabla 9. Entregables de la implementación de los servicios adicionales de seguridad

Entregables de la FASE III. Administración, Operación, Soporte y Mantenimiento de los Servicios Básicos de Seguridad.

Entregables del Servicio Administrado del SOC.

Nombre del Entregable	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse
18. Monitoreo proactivo	Reporte que describe, para la infraestructura tecnológica de seguridad mencionada en el alcance y durante el periodo de operación respectivo, los eventos de actividad sospechosa atendidos. Dentro de este documento se integrará un "Resumen de los incidentes de seguridad presentados durante el periodo". • ID de la Actividad Sospechosa. • Sistema afectado o comprometido. • Origen de la actividad sospechosa. • Severidad. • País del origen de la actividad sospechosa. • Fecha y hora de detección. • Fecha de creación. • Fecha y hora de notificación. • Fecha y hora de envío de dictamen. • Estado. • Dispositivo que lo detecta. • IP del origen de la actividad sospechosa. • Nombre(s) o Direcciones IP(s) . • Patrón de Ataque.	Mensual durante los primeros 7 días naturales de cada mes siguiente al mes vencido y cuando sea identificada una amenaza que ponga en riesgo la operación del "INFONACOT".	Impreso o Electrónico en formato PDF o Word
19. Reporte de Incidentes.	Reporte que enumere los tipos de incidentes detectados y las acciones realizadas para atenderlos. • Soporte a fallas (Distribución de prioridades, Distribución de fallas, Tendencias de fallas presentadas e Indicadores) • Requerimientos (Tipo de solicitudes de Peticiones de Servicio por el usuario, Tendencias de Peticiones de Servicio por el usuario) • Detalle de eventos (Soporte a fallas, Requerimientos) que incluya tiempos de respuesta.	Mensual durante los primeros 7 días naturales de cada mes siguiente al mes vencido y cuando sea identificado un incidente que ponga en riesgo la operación del "INFONACOT".	Impreso o Electrónico en formato PDF o Word
20. Informe o Reporte del Respaldo de Configuraciones de los dispositivos administrados	Se deberá realizar un informe que describa el contenido del respaldo de la configuración y políticas de todos los dispositivos administrados. • Reporte del respaldo de configuraciones y políticas.	Trimestral durante los primeros 7 días naturales del mes siguiente al último periodo vencido	Impreso o Electrónico, almacenados en dispositivos que cuenten con mecanismos de control

Nombre del Entregable	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse
			de acceso seguro.
21. Actualización de las Memorias técnicas	Memorias técnicas actualizadas con los últimos cambios realizados.	Semestral durante los primeros 7 días naturales del mes siguiente al último periodo vencido	Impreso o Electrónico, Microsoft Word y PDF.
22. Correlación y gestión de eventos.	Reporte del servicio de correlación y gestión de eventos. El cual deberá incluir por lo menos la siguiente información: • Disponibilidad del servicio • Detalle de eventos de soporte (fallas y tiempo de solución). • Incidente, No. de ticket, fecha, hora y duración del incidente. • Control de cambios. • Listado, tipos de eventos detectados en el periodo, top 10 de correlación detectados, Reglas de correlación • Severidad de los eventos (eventos por IP destino, eventos correlacionados por IP Origen, eventos correlacionados por Categoría, eventos correlacionados por País, Eventos correlacionados por puerto destino) • Descripción de los eventos de correlación • Listado general de intentos de ataques dirigidos a los portales del "INFONACOT", detectado por cada servicio de seguridad. • Estadísticos de intentos de ataques dirigidos a los portales del "INFONACOT", detectado por los diferentes servicios de seguridad.	Mensual	Impreso o Electrónico en formato PDF o Word
23. Ciberinteligencia	Reporte que describe los hallazgos relacionados con las actividades de ciberinteligencia. • Dominios sospechosos o fraudulentos identificados. • Cuentas de correo institucionales o credenciales comprometidas. • Nivel de riesgo o reputación que tienen asociadas las direcciones IP, dominios y subdominios del "INFONACOT.	Mensual	Impreso o Electrónico en formato PDF o Word

Nombre del Entregable	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse
	• Amenazas avanzadas detectadas conteniendo información sobre los actores, cuáles son sus motivaciones y las Tácticas, Técnicas y Procedimientos (TTP) que utilizan.		
24. Reporte ejecutivo y estadístico	Reporte ejecutivo y estadístico de eventos de seguridad que contenga como mínimo la siguiente información: • Amenazas • Violaciones de políticas de seguridad • Bloqueos • Estado de la seguridad	Mensual	Impreso o Electrónico en formato PDF o Word

Tabla 10. Entregables del Servicio Administrado de SOC

Entregables del Servicio Administrado de Seguridad (Servicios Básicos de Seguridad)

Servicio	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse
27. Protección contra Amenazas Avanzada en Servidores y puntos finales.	Reporte que enumere los eventos relacionados con la protección contra amenazas avanzada en servidores y puntos finales. • Disponibilidad del servicio • Control de cambios. • Permisos aplicados, cambiados o eliminados. • Intentos fallidos de acceso de cuentas en los puntos finales. • Amenazas detectadas en servidores o puntos finales	Mensual	Impreso o Electrónico en formato PDF o Word
28. Gestión de Cuentas con Acceso Privilegiado.	Reporte que enumere los eventos relacionados con la Gestión de Cuentas con Acceso Privilegiado. • Disponibilidad del servicio • Actividad de usuarios. • Inventario de cuentas privilegiadas y sus permisos. • Control de cambios.	Mensual	Impreso o Electrónico en formato PDF o Word
29. Protección Contra Fuga de Información en Punto Final.	Reporte que enumere los eventos relacionados con la Protección Contra Fuga de Información en Punto Final. • Disponibilidad del servicio. • Control de cambios. • Usuarios/puntos finales con mayor nivel de riesgo.	Mensual	Impreso o Electrónico en formato PDF o Word

Tabla 11. Entregables del Servicio Administrado de Seguridad (Servicios Básicos de Seguridad).

Entregables del Servicio Administrado de Protección de Aplicativos.

Servicio	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse
30. Firewall de Aplicaciones Web.	Reporte que enumere los eventos relacionados con el servicio de Firewall de aplicaciones Web. • Disponibilidad del servicio • Control de cambios. • Usuarios y/o Ips bloqueadas. • Intentos de autenticación fallidos. • Trafico malicioso bloqueado • Eventos de seguridad detectados, que incluya la información de origen y método del ataque, dirección IP y localización geográfica del ataque.	Mensual	Impreso o Electrónico en formato PDF o Word
31. Firewall de Bases de Datos.	Reporte que enumere los eventos relacionados con el servicio de Firewall de Bases de datos. • Disponibilidad del servicio • Control de cambios. • Cambios fuera de horas de trabajo. • Cambios en la base de datos de los objetos. • Tipo de conexión realizada a la base de datos. • Información de las conexiones realizadas por cuentas no nombradas que incluya el origen, destino y usuario de S.O.	Mensual	Impreso o Electrónico en formato PDF o Word

Tabla 12. Entregables del Servicio Administrado de Protección de Aplicativos.

Entregables del Servicio de Gestión de Seguridad de la Información.

Servicio	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse

32. Servicio de Gestión de Seguridad de la Información.	Reporte de actividades relacionados con el servicio de gestión de Seguridad de la Información
	• Informe semestral
	  ○ Análisis de riesgos del MGSI
	  ○ Acciones de Mejora
	  ○ Revisión semestral de los controles de seguridad
	• Actuar: Mejora continua
	  ○ Plan de mejora continua del MGSI
		De acuerdo con el plan de trabajo aprobado para el proyecto	Impreso o Electrónico en formato PDF o Word

Tabla 14. Entregables del Servicio de Gestión de Seguridad de la Información.

Entregables de la Mesa de Servicio. *Tabla 15. Entregables de la Mesa de Servicio.*

Entregables del Servicio Administrado de Seguridad Bajo Demanda.

Servicio	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse
34. Análisis de código estático y dinámico.	Reportes de Análisis de código estático y dinámico que incluya como mínimo lo siguiente: • Usuario requirente. • Fecha de solicitud. • Fecha y evidencia de solicitud de análisis • Hallazgos encontrados clasificados por severidad. • Vulnerabilidades encontradas. • Remediaciones propuestas • Conclusiones	Por evento (bajo demanda)	Impreso o Electrónico en formato PDF o Word
35. Protección del Servicio de Verificación de la Credencial para Votar.	Reporte que enumere los eventos relacionados con la Protección del Servicio de Verificación de la Credencial para Votar. • Disponibilidad del servicio • Control de cambios. • Total de transacciones realizadas en el mes. • Total de transacciones por tipo (Aceptado, En Proceso, Rechazado) Total de estampillas de tiempo realizadas.	Mensual	Impreso o Electrónico en formato PDF o Word

Tabla 13. Entregables del Servicio Administrado de Seguridad Bajo Demanda.

Entregables de la FASE IV. Administración, Operación, Soporte y Mantenimiento de los Servicios Adicionales de Seguridad.

Entregables del Servicio Administrado de Seguridad (Servicios Adicionales de Seguridad)

Servicio	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse
39. Filtrado de Contenido Web.	Reporte que enumere los eventos relacionados con el filtrado de contenido WEB de los Usuarios. • Disponibilidad del servicio • Control de cambios. • Estadísticas de la navegación en Internet de los usuarios o grupos de usuarios. • Sitios más visitados. • Aplicaciones más utilizadas. • Usuario con mayor consumo de ancho de banda hacia Internet.	Mensual	Impreso o Electrónico en formato PDF o Word

Servicio	Descripción del Entregable	Periodicidad / fecha de entrega	Formato en que deberá entregarse
	• Malware detectado. • Sitios bloqueados.		
40. Acceso Seguro en el Borde.	Reporte que enumere los eventos relacionados con el servicio de Acceso Seguro en el Borde. • Disponibilidad del servicio • Control de cambios. • Ataques bloqueados. • Malware Detectado • Aplicaciones con mayor uso de ancho de banda. • Usuarios con mayor número de sesiones.	Mensual	Impreso o Electrónico en formato PDF o Word

Tabla 16. Entregables del Servicio Administrado de Seguridad (Adicionales).

Entregables de la FASE V. Plan de Ejecución para lograr la Transición de los Servicios al Vencimiento del Contrato.

Entregable	Descripción	Periodicidad / fecha de entrega	Formato
41. Memorias Técnicas Actualizadas	Memorias técnicas actualizadas con los últimos cambios realizados.	Única vez / Se entregará 15 días naturales previos a la finalización de la vigencia del servicio.	Impreso o Electrónico en formato PDF.
42. Respaldos de las Configuraciones las soluciones tecnológicas que fueron habilitadas administrados.	Respaldos de las configuraciones de las soluciones tecnológicas que fueron habilitadas como parte de los servicios.	Única vez / Se entregará 15 días naturales previos a la finalización de la vigencia del servicio.	Disco de almacenamiento.
43. Base de Conocimiento generada durante las fases de operación.	Base de Conocimiento generada durante las fases de operación.	Única vez / Se entregará 15 días naturales previos a la finalización de la vigencia del servicio.	Formato de BD.
44. Diagrama final de arquitectura	Diagrama final de arquitectura.	Única vez / Se entregará 15 días naturales previos a la finalización de la vigencia del servicio.	Electrónico en formato PDF o Visio.
45. Logs de auditoría de la solución de	Se entregarán los logs de auditoria de la solución de	Única vez / Se entregará 15 días naturales previos	Digital

Entregable	Descripción	Periodicidad / fecha de entrega	Formato
gestión de cuentas de acceso privilegiado	gestión de cuentas de acceso privilegiado del último año.	a la finalización de la vigencia del servicio.	
46 Acta de cierre	El acta de cierre detallará el listado de entregables durante toda la vigencia del contrato, previa satisfacción del "INFONACOT", en forma impresa y en formato electrónico firmado por ambas partes.	Única vez / Se entrega dentro de los primeros 10 días posteriores a la finalización de la vigencia del servicio.	Impreso o Electrónico en formato PDF.

Tabla 17. Entregables para el cierre.

9. PERSONAL ESPECIALIZADO DE "EL LICITANTE".

Como parte de la prestación del "Servicio Administrado de Ciberseguridad" "EL LICITANTE" deberá demostrar que cuenta con personal especializado y calificado para la correcta administración y operación de las herramientas tecnológicas ofertadas para brindar los servicios requeridos en el presenta Anexo Técnico, lo anterior lo deberá demostrar presentando como parte de su propuesta técnica copia simple de las certificaciones vigentes emitidas por los fabricantes de la herramientas propuestas.

El personal propuesto deberá contar con estudios a nivel licenciatura o técnico superior universitario en carreras afines a los servicios requeridos. Lo anterior lo deberá demostrar presentando como parte de su propuesta técnica copia simple del título o cedula que avale el nivel de estudios requeridos.

A continuación, se listan los perfiles que se deberán acreditar como mínimo para la prestación de los servicios, mismos que deberán estar asignados al proyecto para la atención de los servicios y podrán operar a distancia o en sitio de acuerdo a los requerimientos del "INFONACOT".

Administrador del proyecto.

Quien será el encargado de la administración del proyecto desde el inicio de la vigencia hasta la terminación de la misma, Entre sus actividades deberá realizar de manera enunciativa más no limitativa las siguientes:

- Monitorear el cumplimiento de las obligaciones contractuales, del proyecto.
- Identificar desviaciones y riesgos en la implementación.
- Asegurar el cumplimiento técnico y administrativo del contrato.
- Atender las peticiones de cambios, implementaciones, juntas y cualquier solicitud dentro del alcance del contrato por parte del "INFONACOT".
- Realizar consultoría técnica y administrativo del contrato.
- Coordinar la atención a requerimientos y necesidades entre el "INFONACOT" y "EL LICITANTE" que resulte adjudicado.
- Identificar los riesgos de seguridad con bases en los análisis de vulnerabilidades y notificarlos al "INFONACOT".

- Vigilar que los tiempos de atención a solicitudes o incidentes cumplan con los niveles de servicio establecidos

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 3 años de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente como PMP.

Arquitecto de servicios de seguridad informática.

Quien será el encargado de desarrollar y mantener un enfoque arquitectónico de seguridad de información eficaz, asegurando su implementación de acuerdo con las normas y los lineamientos que apliquen al "INFONACOT" deberá estar asignado en las fases I y II y cuando sea requerido derivado de cambios en la arquitectura de los servicios. Entre sus actividades deberá realizar de manera enunciativa más no limitativa las siguientes:

- Supervisar la instalación acorde al diseño arquitectónico propuesto de cada uno de los servicios durante la etapa de implementación.
- Probar las estructuras de seguridad aprovisionadas para garantizar que el comportamiento de estas es el esperado.
- Definir y planear la arquitectura de seguridad de información física, virtual y lógica acorde a los negocios del "INFONACOT".
- Este perfil solo estará asignado durante las fases de implementación de las diferentes soluciones de seguridad informática requeridas en el presente anexo técnico.

Para este perfil "EL LICITANTE" deberá asignar 1 recursos.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 años de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente en CISSP (Certified Information Systems Security Professional).

Líder especialista en servicios de seguridad informática.

Quien será el encargado de coordinar al equipo responsable de la prestación del servicio. Entre sus actividades deberá realizar de manera enunciativa más no limitativa las siguientes:

- Establecer planes de mejora continua para la operación de las tecnologías aprovisionadas.
- Responsable de la gestión y entrega de los servicios de seguridad informática.
- Responsable de monitorear el cumplimiento de los SLA´s establecidos para el proyecto.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 años de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente en CRISC (Certified in Risk an Information Systems Control).

Especialista en Seguridad de la Información.

Quien será el encargado de proponer controles de seguridad de acuerdo con las normas y los lineamientos que apliquen al "INFONACOT". Entre sus actividades deberá realizar de manera enunciativa más no limitativa las siguientes:

- Elaboración de estrategias de seguridad informática y seguridad de la información.
- Elaboración de reportes de Riesgos.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente en CISM (Certified Information Security Manager).

Especialista en monitoreo y análisis de eventos de seguridad informática.

Quien será el encargado de monitorear y analizar los eventos que se generen por las herramientas de seguridad y los reportes que genere el personal designado para la operación de los servicios, relacionados con las alertas de incidentes de Seguridad de la Información. Entre sus actividades deberá realizar de manera enunciativa más no limitativa las siguientes:

- Monitorear los sistemas para detectar actividades inusuales en las diferentes herramientas aprovisionadas como parte de los servicios.
- Realizar análisis de la información recolectada de las diferentes soluciones de seguridad para detectar posibles amenazas de seguridad.
- Realizar investigaciones sobre actividades potencialmente maliciosas identificadas e informarlo al personal responsable para la correcta toma de decisiones y mitigación de estas.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente en ISO 27001 Lead Auditor o Continuous Monitoring Certification (GMON)

Especialista en la herramienta de gestión y correlación de eventos.

Quien será el encargado de la administración, operación y resolución de fallas o problemas relacionados con la herramienta ofertada.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente por parte del fabricante que avale los conocimientos para la administración y configuración de la herramienta tecnológica ofertada.

Especialista en la herramienta de protección contra amenazas avanzadas en servidores y puntos finales.

Quien será el encargado de la administración, operación y resolución de fallas o problemas relacionados con la herramienta ofertada.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente por parte del fabricante que avale los conocimientos para la administración y configuración de la herramienta tecnológica ofertada.

Especialista en la herramienta de Gestión de Cuentas con Acceso Privilegiado.

Quien será el encargado de la administración, operación y resolución de fallas o problemas relacionados con la herramienta ofertada.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente por parte del fabricante que avale los conocimientos para la administración y configuración de la herramienta tecnológica ofertada.

Especialista en la herramienta de Filtrado de contenido Web.

Quien será el encargado de la administración, operación y resolución de fallas o problemas relacionados con la herramienta ofertada.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente por parte del fabricante que avale los conocimientos para la administración y configuración de la herramienta tecnológica ofertada.

Especialista en la herramienta de Protección Contra Fuga de información en el Punto Final.

Quien será el encargado de la administración, operación y resolución de fallas o problemas relacionados con la herramienta ofertada.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente por parte del fabricante que avale los conocimientos para la administración y configuración de la herramienta tecnológica ofertada.

Especialista en la herramienta de Firewall de Aplicaciones Web.

Quien será el encargado de la administración, operación y resolución de fallas o problemas relacionados con la herramienta ofertada.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente por parte del fabricante que avale los conocimientos para la administración y configuración de la herramienta tecnológica ofertada.

Especialista en la herramienta de Firewall de Bases de Datos.

Quien será el encargado de la administración, operación y resolución de fallas o problemas relacionados con la herramienta ofertada.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente por parte del fabricante que avale los conocimientos para la administración y configuración de la herramienta tecnológica ofertada.

Especialista en la solución de Protección del Servicio de Verificación de la Credencial para Votar.

Quien será el encargado de la administración, operación y resolución de fallas o problemas relacionados con la herramienta ofertada.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente por parte del fabricante que avale los conocimientos para la administración y configuración de la herramienta tecnológica ofertada.

Especialista en la herramienta para el Acceso Remoto Seguro.

Quien será el encargado de la administración, operación y resolución de fallas o problemas relacionados con la herramienta ofertada.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente por parte del fabricante que avale los conocimientos para la administración y configuración de la herramienta tecnológica ofertada.

Consultor líder de procesos y cumplimiento en el MGSI.

Quien será el encargado de la revisión de controles tecnológicos conforme al MGSI actual del "INFONACOT". Entre sus actividades deberá realizar de manera enunciativa más no limitativa las siguientes:

- Revisar el cumplimiento de la ejecución de las mejores prácticas de evaluación de riesgos tecnológicos.
- Brindar asesoramiento sobre buenas prácticas de gestión de riesgos y gestión de vulnerabilidades
- Liderar el análisis y evaluación de los riesgos.
- Brindar asesoría sobre gobernanza de datos y gestión de datos.
- Emitir recomendaciones y realiza asesoramiento al cliente respecto a los controles de seguridad.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recurso.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.

- Certificado vigente en CISA (Certified Information Systems Auditor).

Consultor especialista en ISO27001.

Quien será el encargado de revisar y auditar controles de seguridad conforme al MGSI actual del "INFONACOT" y su alcance. Entre sus actividades deberá realizar de manera enunciativa más no limitativa las siguientes:

- Establecer el programa de auditorías de seguridad.
- Desarrollar el programa de auditorías internas.
- Documentar reporte de no conformidades y observaciones durante las auditorías.
- Establecer las acciones de remediación y mejora.
- Brindar recomendaciones basadas en mejores prácticas

Para este perfil "EL LICITANTE" deberá asignar por lo menos uno (1) recursos.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente en ISO/IEC 27001 Lead Auditor.

Personal técnico de la mesa de servicios.

Quienes serán los encargados de la recepción de las solicitudes, incidentes, problemas o requerimientos para la generación del ticket correspondiente. Entre sus actividades deberá realizar de manera enunciativa más no limitativa las siguientes:

- Definir en conjunto con el "INFONACOT" la severidad,
- Consultar la base de datos de conocimiento para brindar una solución o
- Escalarlo al nivel de servicio siguiente para su solución.

Para este perfil "EL LICITANTE" deberá asignar por lo menos un (1) recursos.

Para respaldar los conocimientos y experiencia del personal propuesto para este perfil se deberá presentar copia simple de la siguiente documentación.

- Currículo Vitae en donde se demuestre al menos 1 (un) año de experiencia en tareas similares.
- Copia simple del título y/o cedula que avale los estudios a nivel licenciatura afín a sistemas.
- Certificado vigente en ITI v3 o superior.

9.1. CONSIDERACIONES PARA EL PERSONAL PROPUESTO.

- El personal propuesto deberá cubrir la totalidad de los requerimientos mínimos señalados en la tabla anterior.

- "EL LICITANTE" deberá proporcionar al personal propuesto las herramientas, necesarias para el desempeño de sus funciones y poder garantizar los niveles de servicio especificados en el presente anexo técnico.
- El "INFONACOT" se reserva el derecho de validar la autenticidad de los documentos del personal propuesto por "EL LICITANTE" ante las instancias correspondientes.
- Cuando se requiera hacer un cambio de plantilla "EL LICITANTE" deberá notificarlo al "INFONACOT" con por lo menos 15 días hábiles de antelación y se obliga a reemplazar el personal por otro que cubra el perfil solicitado, para lo cual deberá presentar al "INFONACOT", los documentos que acrediten el cumplimiento de los requisitos solicitados para ese perfil.
- "EL LICITANTE" no podrá reemplazar a más del 30% del personal asignado al proyecto durante la vigencia del contrato, lo anterior considerando que los cambios sean a petición del mismo licitante.
- "INFONACOT" podrá solicitar el cambio de cualquier personal de "EL LICITANTE" en los casos de que no cumpla con las funciones a las que este asignado.

10. VIGENCIA DEL CONTRATO.

La vigencia de la prestación del servicio será a partir del 01/11/2025 al 31/12/2025.

11. LUGAR DE ENTREGA DEL SERVICIO.

"El Proveedor" deberá prestar sus servicios en la Subdirección General de Tecnología de la Información y Comunicación sito en Av. Insurgentes Sur Número 452, Colonia Roma Sur, Alcandía Cuauhtémoc, CP. 06760, Ciudad de México.

En caso de que así lo requiera "El Instituto", el Proveedor deberá prestar su servicio en el edificio, ubicado en Av. Plaza de la República Número 32, Colonia Tabacalera, Alcandía Cuauhtémoc, CP. 06030, Ciudad de México y/o en algunas de las sucursales del Instituto que se ubican en la Ciudad de México.

El Proveedor será responsable de cubrir todos los gastos que se generen del traslado y estancia, de su personal, tanto en oficinas sedes como en sucursales, así como, a los centros de datos con los que cuente el Instituto Fonacot.

12. PENAS CONVENCIONALES Y DEDUCTIVAS.

El "INFONACOT" será responsable del cálculo y aplicación de las penas convencionales y deductivas correspondientes, una vez realizado lo anterior, solicitará a la Dirección de Recursos Materiales y Servicios Generales la validación correspondiente.

El monto de la suma de penas convencionales y deducciones no deberá exceder el 10 % (diez por ciento) del monto total del contrato, una vez transcurridos el supuesto el "INFONACOT" podrá iniciar el procedimiento de recisión administrativa y se hará efectiva la garantía de cumplimiento del mismo.

PENAS CONVENCIONALES

Las penas convencionales que se aplicarán al "LICITANTE" por incumplimiento con el inicio en la prestación del "SERVICIO ADMINISTRADO DE CIBERSEGURIDAD", serán de acuerdo con lo establecido en el artículo 75 de la LAASSP, los artículos 95 y 96 del RLAASSP, así como lo estipulado en el presente Anexo Técnico, de acuerdo con lo siguiente:

El "INFONACOT" aplicará las penas en el siguiente caso:

Penalizaciones FASE I. Implementación de las Soluciones Propuestas para los Servicios Básicos de Seguridad.

Nivel de Servicio	Nivel de Servicio Descripción	Métrica	Penalización
Entrega de Documento	Entrega de Minuta de Reunión de Kick off	Hasta 5 días hábiles posteriores a la fecha de adjudicación del contrato.	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual total, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entrega de Plan de Administración del Proyecto	Hasta 5 días hábiles posteriores a la junta de inicio del proyecto (Kick off).	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual total, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entrega de Reportes de avance del proyecto	Hasta 3 días hábiles posteriores a las reuniones de avance del proyecto.	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual total, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entrega de calendario de Mantenimientos preventivos	Hasta 7 hábiles días después del inicio del contrato	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual total, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entrega de Procedimientos del SOC	Hasta 10 hábiles días después del inicio del contrato	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual total, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entrega de Matriz de riesgos para la implementación del proyecto	Mensualmente durante los primeros 7 días naturales de cada mes siguiente al mes vencido.	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual total, no entregado en los tiempos establecidos en el presente anexo.

Entrega de Documento	Entrega de matriz de escalamiento	Hasta 5 días hábiles posteriores a la fecha de notificación del fallo	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual total, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento.	Entrega de relación del personal asignado al proyecto.	En la primera reunión inicial de las mesas de trabajo.	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual total, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entrega de Memorias técnicas	Diez días hábiles posteriores a la fecha en que concluya la fase de implementación.	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entrega de **p**rocedimientos para la atención a través de la mesa de servicio	Hasta 5 días hábiles posteriores a la fecha de notificación del fallo	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual total, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Acta entrega de Implementación de los servicios de la fase I	Hasta 7 días hábiles de acuerdo al calendario de la terminación de la fase I	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual total, no entregado en los tiempos establecidos en el calendario de fases

Tabla 8. Penalizaciones Fase I

Penalizaciones de la FASE II. Implementación de las Soluciones Propuestas para los Servicios Adicionales de Seguridad.

Nivel de Servicio	Nivel de Servicio Descripción	Métrica	Penalización
Entrega de Documento	Entregable de plan de trabajo para la implementación de las soluciones adicionales de seguridad.	Hasta 5 días hábiles posteriores a la reunión de trabajo.	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual de los servicio de esta fase, no entregado en los

			tiempos establecidos en el presente anexo.
Entrega de Documento	Entregable de reportes de avance de la implementación de las soluciones adicionales de seguridad.	Hasta 3 días hábiles posteriores a las reuniones de avance del proyecto.	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual de los servicio de esta fase, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entregable de matriz de riesgos para la implementación de las soluciones adicionales de seguridad.	Mensualmente durante los primeros 7 días naturales de cada mes siguiente al mes vencido.	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual de los servicio de esta fase, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entregable de memorias técnicas	Diez días hábiles posteriores a la fecha en que concluya la fase de implementación de las soluciones adicionales de seguridad.	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Acta entrega de Implementación de los servicios de la fase II	Hasta 7 días hábiles de acuerdo al calendario de la terminación de la fase II	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual total, no entregado en los tiempos establecidos en el calendario de fases

Penalizaciones de la FASE III. Administración, Operación, Soporte y Mantenimiento de los Servicios Básicos de Seguridad.

Penalización del Servicio Administrado del SOC.

Nivel de Servicio	Nivel de Servicio Descripción	Métrica	Penalización
Entrega de Documento	Entregable de Monitoreo proactivo	Mensual durante los primeros 7 días naturales de cada mes siguiente al	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual

		mes vencido y cuando sea identificada una amenaza que ponga en riesgo la operación del "INFONACOT".	del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entregable de reporte de Incidentes.	Mensual durante los primeros 7 días naturales de cada mes siguiente al mes vencido y cuando sea identificado un incidente que ponga en riesgo la operación del "INFONACOT"..	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entregable de Informe o Reporte del Respaldo de Configuraciones de los dispositivos administrados	Trimestral durante los primeros 7 días naturales del mes siguiente al último periodo vencido	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entregable de actualización de las Memorias técnica	Semestral durante los primeros 7 días naturales del mes siguiente al último periodo vencido	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entregable de reporte del servicio de correlación y gestión de eventos.	Mensual durante los 7 días naturales del mes vencido.	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entregable de Reporte de Ciberinteligencia	Mensual durante los 7 días naturales del mes vencido.	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Reporte ejecutivo y estadístico	Mensual durante los 7 días naturales del mes vencido.	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual

			del servicio, no entregado en los tiempos establecidos en el presente anexo.

Tabla 10. Penalizaciones del Servicio Administrado de SOC

Penalizaciones del Servicio Administrado de Seguridad (Servicios Básicos de Seguridad)

Nivel de Servicio	Nivel de Servicio Descripción	Métrica	Penalización
Entrega de Documento	Reporte de Protección contra Amenazas Avanzada en Servidores y puntos finales.	Mensual	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Reporte de la Gestión de Cuentas con Acceso Privilegiado.	Mensual	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Reporte de Protección Contra Fuga de Información en Punto Final.	Mensual	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.

Tabla 11. Penalizaciones del Servicio Administrado de Seguridad (Servicios Básicos de Seguridad).

Penalización del Servicio Administrado de Protección de Aplicativos.

Nivel de Servicio	Nivel de Servicio Descripción	Métrica	Penalización
Entrega de Documento	Reporte del servicio de Firewall de aplicaciones Web.	Mensual	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no

			entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Reporte del servicio de Firewall de Bases de datos.	Mensual	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Reporte de Análisis de código estático y dinámico.	Mensual	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Reporte del Servicio de Verificación de la Credencial para Votar.	Mensual	0.5 % por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.

Tabla 12. Penalizaciones del Servicio Administrado de Protección de Aplicativos.

Penalizaciones del Servicio Administrado de Seguridad Bajo Demanda.

Nivel de Servicio	Nivel de Servicio Descripción	Métrica	Penalización
Entrega de Documento	Reporte de Análisis de código estático y dinámico.	7 días hábiles después de la terminación del análisis código estático y dinámico.	0.5% por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.

Tabla 13. Penalizaciones del Servicio Administrado de Seguridad Bajo Demanda.

Penalizaciones del Servicio de Gestión de Seguridad de la Información.

Nivel de Servicio	Nivel de Servicio Descripción	Métrica	Penalización
Entrega de Documento	Reporte de actividades relacionados con el servicio de gestión de Seguridad de la Información	7 días hábiles después de la terminación de acuerdo con el plan de trabajo aprobado para el proyecto	0.5% por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.

Tabla 14. Penalización del Servicio de Gestión de Seguridad de la Información.

Penalizaciones de la Mesa de Servicio.

Nivel de Servicio	Nivel de Servicio Descripción	Métrica	Penalización
Entrega de Documento	Entregable de reporte de los tickets recibidos y atendidos durante el periodo.	Mensual	0.5% por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.

Tabla 15. Penalización de la Mesa de Servicio.

Penalizaciones de la FASE IV. Administración, Operación, Soporte y Mantenimiento de los Servicios Adicionales de Seguridad.

Penalizaciones del Servicio Administrado de Seguridad (Servicios Adicionales de Seguridad)

Nivel de Servicio	Nivel de Servicio Descripción	Métrica	Penalización
Entrega de Documento	Entregable de Reporte de filtrado de contenido WEB de los Usuarios.	Mensual	0.5% por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.

Entrega de Documento	Entregable de Reporte del servicio de Acceso Seguro en el Borde.	Mensual	0.5% por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.

Tabla 16. Penalización del Servicio Administrado de Seguridad (Adicionales).

Penalizaciones de la FASE V. Plan de Ejecución para lograr la Transición de los Servicios al Vencimiento del Contrato.

Nivel de Servicio	Nivel de Servicio Descripción	Métrica	Penalización
Entrega de Documento	Entregable de Memorias técnicas actualizadas con los últimos cambios realizados.	Se entregará 15 días naturales previos a la finalización de la vigencia del servicio.	0.5% por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entregable de Respaldos de las configuraciones de las herramientas que fueron habilitadas como parte de los servicios.	Se entregará 15 días naturales previos a la finalización de la vigencia del servicio.	0.5% por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entregable de Base de Conocimiento generada durante las fases de operación.	Se entregará 15 días naturales previos a la finalización de la vigencia del servicio.	0.5% por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entregable de Diagrama final de arquitectura.	Se entregará 15 días naturales previos a la finalización de la vigencia del servicio.	0.5% por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de

			facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Información digital	Entrega de logs de auditoria de la solución de gestión de cuentas con acceso privilegiado	Se entregará 15 días naturales previos a la finalización de la vigencia del servicio.	0.5% por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual del servicio, no entregado en los tiempos establecidos en el presente anexo.
Entrega de Documento	Entregable de acta de cierre.	Se entrega dentro de los primeros 10 días posteriores a la finalización de la vigencia del servicio.	0.5% por cada día natural de atraso, sobre el valor de la factura de antes de IVA del monto de facturación mensual total, no entregado en los tiempos establecidos en el presente anexo.

Tabla 17. Penalizaciones para el cierre.

Tabla: Penalización

Para efectos de la aplicación de las penas convencionales a que se refiere el presente apartado, estas se computarán a partir del día hábil siguiente a aquel en que tuviera que haber sido presentado el entregable y/o servicio.

El "INFONACOT" por ningún motivo autorizará condonaciones de sanciones por atrasos en la entrega del servicio, cuando las causas sean imputables al "LICITANTE".

En los supuestos previstos en el artículo 91, tercer párrafo del RLAASSP, no procederá aplicar al "LICITANTE", penas convencionales por atraso. La modificación del plazo por caso fortuito o fuerza mayor podrá ser solicitada por el "LICITANTE", o por el "INFONACOT".

El pago parcial correspondiente del servicio quedará condicionado, proporcionalmente, al pago que el "LICITANTE" deba efectuar por concepto de penas convencionales, las cuales serán calculadas de conformidad con la Tabla Penalización.

En su caso, cada factura deberá acompañarse del original (para cotejo) y copia simple del comprobante de pago, por concepto de pena convencional que se efectúe a favor de la Tesorería de la Federación, así como de un escrito debidamente firmado por el representante o apoderado legal del "LICITANTE" en el que señale los días de atraso y el monto correspondiente que le fue impuesto por el "Administrador del Contrato" derivado del cálculo de los retrasos en que haya incurrido.

El importe de dicho pago será verificado por el "Administrador del Contrato". En ningún caso las penas convencionales podrán negociarse en especie.

DEDUCCIONES

El "INFONACOT" establece deducciones al pago de servicios con motivo del incumplimiento parcial o deficiente en que pudiera incurrir el "LICITANTE", respecto al "SERVICIO ADMINISTRADO DE CIBERSEGURIDAD", objeto del presente Anexo Técnico, para lo cual se establecerán los límites del incumplimiento a partir del cual se iniciará el proceso de recisión administrativa en los términos de los artículos 76 y 77 de la LAASSP y el artículo 97 del Reglamento de la LAASSP, conforme a lo establecido en el Anexo Técnico.

Las deducciones al pago del servicio previstas en el presente punto serán determinadas en función de los servicios prestados de manera parcial o deficiente. Dichas deducciones deberán calcularse hasta la fecha en que materialmente se cumpla la obligación y sin que cada concepto de deducciones exceda del 10 % (diez por ciento) del monto total del contrato una vez rebasado se deberá iniciar el procedimiento administrativo de rescisión correspondiente. Los montos para deducir se deberán aplicar en la factura que el "LICITANTE" presente para su cobro, inmediatamente después de que el "INFONACOT" tenga cuantificada la deducción correspondiente.

Cabe señalar que todas aquellas regulaciones que no estén consideradas en estas penas se tratarán conforme a lo establecido en la LAASSP y el RLAASSP, así como en cualquier otra disposición normativa que emita la Secretaría de la Función Pública.

Los criterios para la aplicación de las deducciones serán a partir del primer día hábil de etapa de operación de acuerdo con el requerimiento, como se muestra a continuación:

Deductivas.

Nivel de Servicio	Nivel de Servicio Descripción	Métrica	Deductivas
Disponibilidad de las soluciones tecnológicas de seguridad de los servicios de seguridad informática	Disponibilidad en cada uno de las soluciones tecnológicas de los servicios	**99.9%**	3 al millar por cada minuto de indisponibilidad sobre el monto total del costo mensual del servicio al que aplica, o en su caso el tiempo proporcional
Disponibilidad del servicio del SOC	Monitoreo 7x24x365	**99.9%**	2 al millar por cada hora de indisponibilidad sobre costo mensual del servicio, o en su caso el tiempo proporcional
Monitoreo y notificación de actividad sospechosa	Tiempo promedio de notificación de la actividad sospechosa (AS) identificada a través de la infraestructura de seguridad	Que la notificación de actividad sospechosa se realice en un tiempo máximo de 30 minutos	Se aplicará la deductiva de 3 al millar por cada minuto de atrasado en su entrega sobre

			el importe mensual del servicio
Diagnóstico inicial de Incidencia de Seguridad	Tiempo en minutos operativos a partir de la asignación del ticket para obtener y notificar el diagnóstico inicial de seguridad	Tiempo máximo 60 minutos.	Se aplicará la deductiva de 2 al millar por cada minuto de atrasado en su entrega sobre el importe mensual del servicio
Solución de incidencia de seguridad	Tiempo en minutos de la solución de una incidencia de seguridad con las soluciones tecnológicas utilizadas en los servicios del presente anexo de acuerdo a la criticidad asignada: Alta Media Baja	Tiempo máximo de solución de acuerdo a la criticidad: Alta: 120 minutos Media:240 minutos Baja:560 minutos	Se aplicará la deductiva de 2 al millar por cada minuto de atrasado en su entrega sobre el importe mensual del servicio
Altas, Bajas y Cambios	Tempo máximo en las altas, bajas, cambios en los dispositivos de seguridad. Dependiendo de cada servicio y la cantidad de altas, bajas y cambios	Servicio de Protección contra Amenazas Avanzada en Servidores y puntos finales: 1 a 3 equipos: 120 minutos 4 a 10 equipos: 240 minutos 11 a 50 equipos: 3 días Servicio de Protección Contra Fuga de Información: 1 a 3 equipos: 120 minutos 4 a 10 equipos: 240 minutos 11 a 50 equipos: 3 días Servicio de Gestión de Cuentas con Acceso Privilegiado.: 1 a 3 equipos: 120 minutos 4 a 10 equipos: 240 minutos 11 a 20 equipos: 3 días Servicio de Firewall de Bases de datos: 1 base de datos: 3 días	Se aplicará la deductiva de 2 al millar por cada minuto de atrasado en su entrega sobre el importe mensual del servicio

		Servicio de Firewall de Aplicaciones: 1 aplicación: 3 días Acceso Seguro en el Borde aplicación de políticas: 1 a 3 políticas: 120 minutos 4 a 10 políticas: 240 minutos 11 a 30 políticas: 3 días Servicio de Filtrado de contenido aplicación de políticas: 1 a 3 políticas: 120 minutos 4 a 10 políticas: 240 minutos 11 a 30 políticas: 3 días	
Análisis de seguridad de código estático y dinámico	Tiempo máximo en el análisis de la aplicación	Tiempo máximo de análisis de acuerdo al número de líneas: 1-100,000 líneas de código: 5 días hábiles. 100,001 a 500,000 líneas de código: 10 días hábiles 500,001 a 1,000,000 líneas de código: 15 días hábiles	Se aplicará la deductiva de 2 al millar por cada minuto de atrasado en su entrega sobre el importe mensual del servicio

13. TRANSICIÓN DEL SERVICIO.

El proveedor se deberá comprometer en su propuesta a que; al finalizar el contrato, quedará en propiedad del INSTITUTO todo el hardware y software contemplado dentro del alcance a título gratuito sin condición alguna al final del contrato.

14. PROPUESTA ECONÓMICA.

SERVICIOS	UNIDAD DE MEDIDA	UNIDADES TOTALES (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO TOTAL AxB
Servicio de Gestión de Seguridad de la Información	MES DE SERVICIO	2	$	$
PRECIOS TOTALES ANTES DE IVA			**$**	**$**
IVA			**$**	**$**
PRECIOS TOTALES INCLUYENDO IVA			**$**	**$**

El licitante deberá considerar 2 meses de servicio para la elaboración de su propuesta económica.

SERVICIOS	UNIDAD DE MEDIDA	CANTIDAD MÍNIMA MENSUAL (A)	CANTIDAD MÁXIMA MENSUAL (B)	PRECIO UNITARIO MENSUAL (C)	PRECIO MÍNIMOS (AxCx23)	PRECIO MÁXIMOS (BxCx23)
Servicio Administrado de SOC						
Correlación y Gestión de eventos	EPS	1500	2500	$	$	$
Ciberinteligencia	Dominios	1	2	$	$	$
	Cuentas y/o usuarios expuestos	1	10	$	$	$
PRECIOS TOTALES ANTES DE IVA					**$**	**$**
IVA					**$**	**$**
PRECIOS TOTALES INCLUYENDO IVA					**$**	**$**

EL LICITANTE DEBERÁ CONSIDERAR 2 MESES DE SERVICIO PARA LA ELABORACIÓN DE SU PROPUESTA ECONÓMICA.

Servicio Administrado de Seguridad	UNIDAD DE MEDIDA	CANTIDAD MÍNIMA MENSUAL (A)	CANTIDAD MÁXIMA MENSUAL (B)	PRECIO UNITARIO MENSUAL (C)	PRECIO MÍNIMOS AxCx23	PRECIO MÁXIMOS BxCx23
Protección contra amenazas avanzadas en servidores y puntos finales	Servidor o punto final	1200	2000	$	$	$
Gestión de cuentas con acceso privilegiado	Activos	200	350	$	$	$
Filtrado de contenido web	Usuario	1200	1600	$	$	$
Protección contra fuga de información	Punto final	1200	1600	$	$	$
				PRECIOS TOTALES ANTES DE IVA	**$**	**$**
				IVA	**$**	**$**
				PRECIOS TOTALES INCLUYENDO IVA	**$**	**$**

EL LICITANTE DEBERÁ CONSIDERAR 2 MESES DE SERVICIO PARA LA ELABORACIÓN DE SU PROPUESTA ECONÓMICA.

Acceso Seguro en el Borde	UNIDAD DE MEDIDA	CANTIDAD MÍNIMA MENSUAL (A)	CANTIDAD MÁXIMA MENSUAL (B)	PRECIO UNITARIO MENSUAL (C)	PRECIO MÍNIMOS AxCx23	PRECIO MÁXIMOS BxCx23
Equipo modelo A	Equipo	1	5	$	$	$
Equipo modelo B	Equipos	0	3	$	$	$
Equipo modelo C	Equipos	0	3	$	$	$
				PRECIOS TOTALES ANTES DE IVA	**$**	**$**
				IVA	**$**	**$**
				PRECIOS TOTALES INCLUYENDO IVA	**$**	**$**

EL LICITANTE DEBERÁ CONSIDERAR 2 MESES DE SERVICIO PARA LA ELABORACIÓN DE SU PROPUESTA ECONÓMICA.

Servicio Administrado de Protección de Aplicativos.	UNIDAD DE MEDIDA	CANTIDAD MÍNIMA MENSUAL (A)	CANTIDAD MÁXIMA MENSUAL (B)	PRECIO UNITARIO MENSUAL (C)	PRECIO MÍNIMOS AxCx23	PRECIO MÁXIMOS BxCx23
Firewall de aplicaciones web	Aplicaciones Web	10	30	$	$	$
Firewall de base de datos	Base de datos	30	60	$	$	$
				PRECIOS TOTALES ANTES DE IVA	$	$
				IVA	$	$
				PRECIOS TOTALES INCLUYENDO IVA	$	$

CADA SERVICIO SERÁ PAGADO EN EL MES EN QUE SEA CONSUMIDO.

Servicio Administrado de Seguridad Bajo Demanda.	UNIDAD DE MEDIDA	CANTIDAD MÍNIMA MENSUAL (A)	CANTIDAD MÁXIMA MENSUAL (B)	PRECIO UNITARIO (C)	PRECIO MÍNIMOS AxC	PRECIO MÁXIMOS BxC
Análisis de código estático y dinámico	Evento	0	2	$	$	$
				PRECIOS TOTALES ANTES DE IVA	$	$
				IVA	$	$
				PRECIOS TOTALES INCLUYENDO IVA	$	$

EL LICITANTE DEBERÁ CONSIDERAR 2 MESES DE SERVICIO PARA LA ELABORACIÓN DE SU PROPUESTA ECONÓMICA.

Servicio Administrado de Seguridad Bajo Demanda.	UNIDAD DE MEDIDA	CANTIDAD MÍNIMA MENSUAL (A)	CANTIDAD MÁXIMA MENSUAL (B)	PRECIO UNITARIO MENSUAL (C)	PRECIO MÍNIMOS AxCx23	PRECIO MÁXIMOS BxCx23
Protección del Servicio de Verificación de la Credencial para Votar.	Servicio	0	1	$	$	$
PRECIOS TOTALES ANTES DE IVA				**$**	**$**	**$**
IVA				**$**	**$**	**$**
PRECIOS TOTALES INCLUYENDO IVA				**$**	**$**	**$**

Nota: En la tabla de la propuesta económica se deberá poner las cantidades en número y en texto en pesos mexicanos

NORMAS, POLÍTICAS Y LINEAMIENTOS INSTITUCIONALES

Será aplicable para el presente contrato, la Ley de Adquisiciones, Arrendamiento y Servicio del Sector Público y su Reglamento; Código Civil Federal; Ley Federal de Procedimiento Administrativo; Código Federal de Procedimientos Civiles; Ley Federal de Presupuesto y Responsabilidad Hacendaria, el Marco de Gestión de Seguridad de la Información y demás disposiciones aplicables.

15. GARANTÍA DE CUMPLIMIENTO

Para garantizar el cumplimiento del contrato "EL LICITANTE", se obliga a entregar dentro de los 10 (diez) días naturales siguientes a la fecha de firma del instrumento contractual, garantía divisible en moneda nacional (pesos mexicanos) por el equivalente al 10% (diez por ciento) del importe del contrato, sin considerar el impuesto al valor agregado, la cual deberá emitir conforme a los lineamientos de "INFONACOT" para cumplir con los requisitos establecidos en el artículo 103 del Reglamento de la LAASSP, aplicable en la materia.

16. ADMINISTRADOR DEL CONTRATO

El administrador del contrato será el responsable de calcular y notificar al Proveedor las penas convencionales y las deductivas que se hubieran determinado en la recepción del bien y/o prestación del servicio. Para la recepción del bien o servicio el Administrador del contrato verificará el cumplimiento de las características técnicas requeridas en el presente anexo técnico, de conformidad con lo establecido en el penúltimo párrafo del artículo 84 del Reglamento de la LAASSP.

Ciudad de México, octubre de 2025

Autorizó

Ing. Ricardo Oria Esquivel
Subdirector General de Tecnologías de la Información y Comunicación, y encargado de llevar a cabo las funciones inherentes al cargo de Oficial de Seguridad de la Información en el Instituto FONACOT, designado mediante oficio No. DG/048/2025

Elaboró

Lic. Gerardo Daza López
Subdirector de Infraestructura Tecnológica, y personal de apoyo para el debido cumplimiento de las funciones al cargo de Oficial de Seguridad de la Información en el Instituto FONACOT, designado mediante oficio No. SGTIC.402.06.2025

17. GLOSARIO DE TÉRMINOS.

Activo. - Los programas de cómputo, bienes informáticos, soluciones tecnológicas, sistemas o aplicativos, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.

Activos Críticos. - Los programas de cómputo, bienes informáticos, soluciones tecnológicas, sistemas o aplicativos, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos que son de vital importancia para mantener las operaciones de una organización.

AD.- (siglas – Active Directory) servicio de directorio en una red distribuida.

AES.- (siglas - Advanced Encryption Standard) también conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

Amenaza. - Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Desde el punto de vista de una organización pueden ser tanto internas como externas.

Amenaza Avanzada. - Es un ciberataque dirigido a una entidad en concreto, que emplea diferentes recursos, como malware, ataques de ingeniería social o vulnerabilidades desconocidas, incluso recursos diseñados específicamente para atacar el objetivo seleccionado, entre otros con el fin de permanecer dentro de los sistemas del objetivo todo el tiempo que estime necesarios para alcanzar sus propósitos.

Antivirus.- Son programas que buscan prevenir, detectar y eliminar virus informáticos.

Antimalware - Protección contra software malicioso.

Antispam.- solución de software que permite a los usuarios prevenir o restringir la entrega de spam (correos no deseados). Analiza automáticamente todos los correos electrónicos entrantes enviados a un buzón de correo

BCP. - Business Continuity Planning. Plan de continuidad del Negocio, el cual permite definir las medidas a adoptar para mantener la continuidad de las operaciones en caso de alguna afectación.

BIA - Business Impact Analysis - Análisis de impacto al negocio.

CISA. - (siglas - Certified Information Systems Auditor) es una certificación para auditores respaldada por la Asociación de Control y Auditoría de Sistemas de Información (ISACA) (Information Systems Audit and Control Association).

CISSP.- (siglas - Certified Information Systems Security Professional) es un profesional en aseguramiento de la información que define la arquitectura, diseño, administración y/o controles que garantizan la seguridad.

CPU. - (siglas - Central Processing Unit) es la parte central de toda computadora ya que es la que cumple la tarea de procesamiento de todas las funciones, así como también de almacenamiento de la información.

Cuentas privilegiadas. - Son cuentas que se emplean en sistemas o aplicaciones y que tienen permisos elevados, que además de poder visualizar la información a la que tienen acceso, pueden modificarla o modificar la configuración de los sistemas o aplicaciones.

Dashboard.- Son tableros de control que le permiten a una organización visualizar la información más importante para monitorear, analizar y administrar el desempeño del negocio de manera más efectiva.

DBA - Administrador de Base de Datos.

DDoS. - (siglas - Distributed Denial of Service) ataque distribuido de denegación de servicio.

DoS. - (siglas – Denial of Service) Negación de servicio.

DES. - (siglas - Data Encryption Standard) Desarrollado por IBM, es un algoritmo de cifrado que utiliza bloques de datos de 64 bits y clave de 56 bits.

DHCP.- (siglas - Dinamic Host Control Protocol) Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular).

DLP - Prevención de fuga de Información.

DNS. - (siglas - Domain Name System) sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios.

DRP. - Disaster Recovery Planning.

Endpoint - Punto Final / Usuario Final.

Firewall. - Es un dispositivo físico o virtual que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.

FTP.- (siglas - File Transfer Protocol) es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente servidor.

HIPS - Sistema de prevención de intrusiones basado en el Host.

HTTP.- (siglas - HyperText Transfer Protocol) es el método más común de intercambio de información en la world wide web, el método mediante el cual se transfieren las páginas web a un ordenador.

Incidente o Incidente de ciberseguridad. - Es un evento o serie de eventos inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio; provocando una pérdida o uso indebido de información, interrupción parcial o total de los Sistemas.

Internet.- Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen funciones como una red lógica única de alcance mundial.

IP spoofing.- en términos de seguridad de redes hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

IP.- (siglas – Internet Protocol) estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes conmutados.

IPS.- (siglas – Intrusion Prevention Systems) sistema de prevención de intrusiones.

IPsec.- (siglas - Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

IPv4.- es la versión 4 del Protocolo de Internet (IP o Internet Protocol) y constituye la primera versión de IP que es implementada de forma extensiva.

ISO/IEC.- (siglas – International Organization for Standardizacion/ International Electrotechnical Commission) es un estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional.

ITIL.- (siglas - Information Technology Infrastructure Library) La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL, es un conjunto de conceptos y buenas prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general.

LAN.- (siglas – Local Area Network) Red de Área Local.

Latencia.- suma de retardos temporales dentro de una red.

LDAP - Protocolo Ligero/Simplificado de Acceso a Directorios.

MPLS.- (siglas – Multiprotocol Label Switching) Están compuestas de un gran número de routers interconectados comerciales, gubernamentales, universitarios y otros de gran capacidad que llevan los datos a través de países, continentes y océanos del mundo mediante cables de fibra óptica.

NAT.- (siglas – Network Address Translation) El proceso de la traducción de direcciones de red, se desarrolló en respuesta a la falta de direcciones de IP con el protocolo IPv4.

OLA. - (siglas - Operational Level Agreement) Acuerdos de Niveles de Operación.

OSPF. - (siglas – Open Shortest Path First) protocolo de encaminamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo SmoothWall Dijkstra enlace estado (LSE Link State Algorithm) para calcular la ruta idónea entre dos nodos cualesquiera de un sistema autónomo.

P2P.- (siglas – Peer to Peer) es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

PHP.- (siglas - Hypertext Preprocessor) es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML.

PMBOK - Guía de los fundamentos para la dirección de proyectos.

PMI - El Project Management Institute.

PMP. - Project Management Professional.

Proxy.- es un servidor programa o dispositivo, que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C).

Puerto USB.- (siglas - Universal Serial Bus) una clase de conexión que posibilita el envío y la recepción de información.

QoS.- (siglas – Quality of Services) En el campo de las redes de computadoras y otras redes de telecomunicación en paquetes, los términos de ingeniería del tráfico se refieren a mecanismos de control para la reserva de recursos en vez de la calidad de servicio lograda.

Rack.- es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones.

RFC.- (siglas - Request for Comments) son una serie de publicaciones del grupo de trabajo de ingeniería de internet que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos.

Sandbox. - un sistema de aislamiento de procesos o entorno aislado, a menudo usado como medida de seguridad.

SD-WAN.- es un acrónimo de redes definidas por software en una red de área amplia (WAN). SD-WAN simplifica la administración y el funcionamiento de una WAN al desacoplar (separar) el hardware de red de su mecanismo

de control. Este concepto es similar a cómo la red definida por software implementa la tecnología de virtualización para mejorar la administración y operación del centro de datos. Una aplicación clave de SD-WAN es permitir a las empresas construir WAN de mayor rendimiento utilizando un acceso a Internet de menor costo y disponible comercialmente, lo que permite a las organizaciones reemplazar parcial o totalmente las tecnologías de conexión WAN privadas más caras, como MPLS.

Seguridad Informática. - Se define como una capa de protección para los activos de información, a partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo.

SI. - Seguridad de la Información.

SIEM. - (siglas - Security Information and Event Management) la gestión de eventos e información de seguridad.

Site.- es un lugar o especio cerrado donde se encuentran los equipos de comunicaciones (Router CPE, Switches, Servidores, etc.)

SNMPv3.- (siglas - Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

SLA. - (siglas - service-level agreement) es un acuerdo escrito entre un proveedor de servicio y el INFONACOT con objeto de fijar el nivel acordado para la calidad de los servicios contratados.

SOC.- (siglas - Security Operations Center) Centro de Operaciones de Seguridad.

Spyware.- programa espía es un malware que recopila información de un ordenador y después transmite esta información a una entidad externa.

SQL.- (siglas - Structured Query Language) es el lenguaje estándar ANSI/ISO de definición, manipulación y control de bases de datos relacionales. Es un lenguaje declarativo: sólo hay que indicar qué se quiere hacer. En cambio, en los lenguajes procedimentales es necesario especificar cómo hay que hacer cualquier acción sobre la base de datos.

Stored Procedure - Procedimiento almacenado (Base de Datos).

Switch.- dispositivo de interconexión de redes informáticas.

Takeover. - Se refiera a las actividades relacionadas a tomar el control sobre la operación de las soluciones tecnológicas que se encuentran actualmente instaladas y operando.

Tiempo de atención. – Es el tiempo que transcurre cuando el personal de la mesa de ayuda o un ingeniero de soporte recibe la notificación de una solicitud, incidente, problema o requerimiento hasta que inicia las acciones para su solución

Tiempo de resolución. – Es el tiempo que transcurre cuando el personal de la mesa de ayuda o un ingeniero de soporte inicia las acciones de solución y obtiene un diagnóstico para la resolución.

Throughput.- En redes de comunicaciones, como Ethernet, se llama throughput a la tasa promedio de éxito en la entrega de un mensaje sobre un canal de comunicación. Este dato puede ser entregado sobre un enlace físico o lógico, o a través de un cierto nodo de la red. Por regla general, el throughput es medido en bits por segundo (bit/s o bps), y a veces en paquetes de datos por segundo o paquetes de datos por franja de tiempo.

TIC. - Tecnologías de la Información y Comunicaciones.

URL.- (siglas - Uniform Resource Locator) Localizador Uniforme de Recursos, se trata de la secuencia de caracteres que sigue un estándar y que permite denominar recursos dentro del entorno de Internet para que puedan ser localizados.

VPN. - (siglas - Virtual Private Network) Red Privada Virtual.

WAN.- (siglas – Wide Area Network) El concepto se utiliza para nombrar a la red de computadoras que se extiende en una gran franja de territorio, ya sea a través de una ciudad, un país o, incluso, a nivel mundial. Un ejemplo de red WAN es la propia Internet.

WEB.- El concepto se utiliza en el ámbito tecnológico para nombrar a una red informática y, en general, a Internet

ANEXO II
Cotización

Ciudad de México a 01 de octubre de 2025.

Asunto: Respuesta a **Oficio No. SGTIC.629.10.2025**
Asunto: Investigación de Mercado para nueva contratación.

INSTITUTO FONACOT
ING. RICARDO ORIA ESQUIVEL
SUBDIRECTOR GENERAL DE TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIÓN

Trabajo y Previsión Social | fonacot

02 OCT. 2025
11:56 hrs
Recibido
Subdirección General de Tecnologías de la Información y Comunicación

P R E S E N T E .

La suscrita **Yolanda Saldaña Tavera**, en mi carácter de **Representante Legal** de la persona moral **IQSEC, S.A. DE C.V.**, a nombre de mi representada, por este medio doy respuesta formal al oficio **Núm. SGTIC.629.10.2025** de fecha **1º de octubre de 2025**.

Me refiero al Contrato Plurianual Abierto para la Prestación del **Servicio Administrado de Seguridad Informática No. FNCOT/LP/025/2023** y su último Convenio Modificatorio **No. FNCOT/LP/025-4/2023** que tiene mi representada con este Instituto con una vigencia del 17 de marzo de 2023 al 31 de octubre de 2025, por lo anteriormente expuesto, por este medio respetuosamente manifiesto que:

En respuesta a la investigación de mercado convocada por el Instituto, hago de su conocimiento que mi representada **sí se encuentra** en posibilidades técnicas, administrativas y económicas de otorgar los mismos servicios en iguales condiciones en cuanto a precio, características y calidad de los servicios en materia del Contrato **No. FNCOT/LP/025/2023** y su último Convenio Modificatorio **No. FNCOT/LP/025-4/2023** denominado **"Servicio Administrado de Seguridad Informática"** para la celebración de un nuevo contrato denominado **"Servicio Administrado de Ciberseguridad"**, con una **vigencia del 01 de noviembre al 31 de diciembre de 2025,** ratificando las características técnicas.

Para efectos de la evaluación en comento, mi representada presenta la siguiente propuesta económica, la cual contempla la totalidad de los servicios solicitados, por un periodo de dos meses, la cual tiene una vigencia de 120 días naturales a partir de la fecha de su presentación.

SERVICIOS	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Servicio Administrado de SOC				
Correlación y Gestión de eventos	EPS	2500	198.00	990,000.00
Ciberinteligencia	Dominios	2	38,581.00	154,324.00
	Cuentas y/o usuarios expuestos	10	7,716.00	154,320.00
			PRECIOS TOTALES ANTES DE IVA	1,298,644.00
			IVA	207,783.04
			PRECIOS TOTALES INCLUYENDO IVA	1,506,427.04

Servicio Administrado de Seguridad	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Protección contra amenazas avanzadas en servidores y puntos finales	Servidor o punto final	2000	235.00	940,000.00
Gestión de cuentas con acceso privilegiado	Activos	350	1,307.00	914,900.00
Filtrado de contenido web	Usuario	1600	337.00	1,078,400.00
Protección contra fuga de información	Punto final	1600	169.00	540,800.00
			PRECIOS TOTALES ANTES DE IVA	3,474,100.00
			IVA	555,856.00
			PRECIOS TOTALES INCLUYENDO IVA	4,029,956.00

Acceso Seguro en el Borde	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Equipo modelo A	Equipo	5	218,912.00	2,189,120.00
Equipo modelo B	Equipos	3	18,935.00	113,610.00
Equipo modelo C	Equipos	3	18,935.00	113,610.00
			PRECIOS TOTALES ANTES DE IVA	2,416,340.00
			IVA	386,614.40
			PRECIOS TOTALES INCLUYENDO IVA	2,802,954.40

Servicio Administrado de Protección de Aplicativos	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Firewall de aplicaciones web	Aplicaciones Web	30	5,850.00	351,000.00
Firewall de base de datos	Base de datos	60	29,676.00	3,561,120.00
			PRECIOS TOTALES ANTES DE IVA	3,912,120.00
			IVA	625,939.20
			PRECIOS TOTALES INCLUYENDO IVA	4,538,059.20

Servicio Administrado de Seguridad Bajo Demanda	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Análisis de código estático y dinámico	Evento	2	44,792.00	179,168.00
			PRECIOS TOTALES ANTES DE IVA	179,168.00
			IVA	28,666.88
			PRECIOS TOTALES INCLUYENDO IVA	207,834.88

Servicio Administrado de Seguridad Bajo Demanda	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Protección del Servicio de Verificación de la Credencial para Votar	Hardware (Equipos)	1	259,090.00	518,180.00
			PRECIOS TOTALES ANTES DE IVA	518,180.00
			IVA	82,908.80
			PRECIOS TOTALES INCLUYENDO IVA	601,088.80

SERVICIOS	UNIDAD DE MEDIDA	UNIDADES TOTALES (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO TOTAL (AxB)
Servicio de Gestión de Seguridad de la Información	MES DE SERVICIO	2	402,977.00	805,954.00
			PRECIOS TOTALES ANTES DE IVA	805,954.00
			IVA	128,952.64
			PRECIOS TOTALES INCLUYENDO IVA	934,906.64

RESUMEN DE LA PROPUESTA ECONÓMICA	
SERVICIO	**SUMA DE LOS PRECIOS TOTALES DE TODAS LAS TABLAS**
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DE SEGURIDAD INFORMÁTICA	**12,604,506.00**
PRECIOS TOTALES ANTES DE IVA	**12,604,506.00**
IVA	**2,016,720.96**
PRECIOS TOTALES INCLUYENDO IVA	**14,621,226.96**

Monto en Letra Precio mínimo: N/A
Monto en Letra Precio máximo: $12,604,506.00 M.N. (Doce millones seiscientos cuatro mil quinientos seis pesos 00/100 MXN), antes de IVA
Datos de contacto:
Correo: infolicitaciones@iqsec.com.mx
Número Telefónico: 55-4163-1700
Vigencia de Cotización: 60 días naturales

Finalmente, ratifico que mi representada se encuentra en posibilidades técnicas, administrativas y económicas de otorgar los mismos servicios en iguales condiciones en cuanto precio, características y calidad de los servicios en materia del contrato **No. FNCOT/LP/025/2023** denominado **"Servicio Administrado de Seguridad Informática"** y su último convenio Modificatorio **No. FNCOT/LP/025-4/2023** para la celebración de un nuevo Contrato con vigencia del **1 de noviembre al 31 de diciembre de 2025.**

Sin otro particular por el momento, aprovecho la oportunidad para enviarle un cordial saludo.

A T E N T A M E N T E

Yolanda Saldaña Tavera
Representante Legal
IQSEC, S.A. DE C.V.

Servicio Administrado de Protección de Aplicativos	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Firewall de aplicaciones web	Aplicaciones Web	30	5,850.00	351,000.00
Firewall de base de datos	Base de datos	60	29,676.00	3,561,120.00
			PRECIOS TOTALES ANTES DE IVA	3,912,120.00
			IVA	625,939.20
			PRECIOS TOTALES INCLUYENDO IVA	4,538,059.20

Servicio Administrado de Seguridad Bajo Demanda	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Análisis de código estático y dinámico	Evento	2	44,792.00	179,168.00
			PRECIOS TOTALES ANTES DE IVA	179,168.00
			IVA	28,666.88
			PRECIOS TOTALES INCLUYENDO IVA	207,834.88

Servicio Administrado de Seguridad Bajo Demanda	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Protección del Servicio de Verificación de la Credencial para Votar	Hardware (Equipos)	1	259,090.00	518,180.00
			PRECIOS TOTALES ANTES DE IVA	518,180.00
			IVA	82,908.80
			PRECIOS TOTALES INCLUYENDO IVA	601,088.80

SERVICIOS	UNIDAD DE MEDIDA	UNIDADES TOTALES (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO TOTAL (AxB)
Servicio de Gestión de Seguridad de la Información	MES DE SERVICIO	2	402,977.00	805,954.00
			PRECIOS TOTALES ANTES DE IVA	805,954.00
			IVA	128,952.64
			PRECIOS TOTALES INCLUYENDO IVA	934,906.64

RESUMEN DE LA PROPUESTA ECONÓMICA	
SERVICIO	**SUMA DE LOS PRECIOS TOTALES DE TODAS LAS TABLAS**
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DE SEGURIDAD INFORMÁTICA	**12,604,506.00**
PRECIOS TOTALES ANTES DE IVA	**12,604,506.00**
IVA	**2,016,720.96**
PRECIOS TOTALES INCLUYENDO IVA	**14,621,226.96**

Monto en Letra Precio mínimo: N/A
Monto en Letra Precio máximo: $12,604,506.00 M.N. (Doce millones seiscientos cuatro mil quinientos seis pesos 00/100 MXN), antes de IVA
Datos de contacto:
Correo: infolicitaciones@iqsec.com.mx
Número Telefónico: 55-4163-1700
Vigencia de Cotización: 60 días naturales

Finalmente, ratifico que mi representada se encuentra en posibilidades técnicas, administrativas y económicas de otorgar los mismos servicios en iguales condiciones en cuanto precio, características y calidad de los servicios en materia del contrato **No. FNCOT/LP/025/2023** denominado **"Servicio Administrado de Seguridad Informática"** y su último convenio Modificatorio **No. FNCOT/LP/025-4/2023** para la celebración de un nuevo Contrato con vigencia del **1 de noviembre al 31 de diciembre de 2025.**

Sin otro particular por el momento, aprovecho la oportunidad para enviarle un cordial saludo.

A T E N T A M E N T E

Yolanda Saldaña Tavera
Representante Legal
IQSEC, S.A. DE C.V.

Subdirección General de Tecnologías de la Información y Comunicación
Oficio No. SGTIC.629.10.2025
Asunto: Investigación de Mercado para nueva contratación.

Ciudad de México, a 01 de octubre de 2025.

INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES

FORMATO DE COTIZACION PARA EL SERVICIO ADMINISTRADO DE CIBERSEGURIDAD.

SERVICIOS	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Servicio Administrado de SOC				
Correlación y Gestión de eventos	EPS	2500	198.00	990,000.00
Ciberinteligencia	Dominios	2	38,581.00	154,324.00
	Cuentas y/o usuarios expuestos	10	7,716.00	154,320.00
			PRECIOS TOTALES ANTES DE IVA	1,298,644.00
			IVA	207,783.04
			PRECIOS TOTALES INCLUYENDO IVA	1,506,427.04

Servicio Administrado de Seguridad	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Protección contra amenazas avanzadas en servidores y puntos finales	Servidor o punto final	2000	235.00	940,000.00
Gestión de cuentas con acceso privilegiado	Activos	350	1,307.00	914,900.00
Filtrado de contenido web	Usuario	1600	337.00	1,078,400.00
Protección contra fuga de información	Punto final	1600	169.00	540,800.00
			PRECIOS TOTALES ANTES DE IVA	3,474,100.00
			IVA	555,856.00
			PRECIOS TOTALES INCLUYENDO IVA	4,029,956.00

Acceso Seguro en el Borde	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Equipo modelo A	Equipo	5	218,912.00	2,189,120.00
Equipo modelo B	Equipos	3	18,935.00	113,610.00
Equipo modelo C	Equipos	3	18,935.00	113,610.00
			PRECIOS TOTALES ANTES DE IVA	2,416,340.00
			IVA	386,614.40
			PRECIOS TOTALES INCLUYENDO IVA	2,802,954.40

Servicio Administrado de Protección de Aplicativos	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Firewall de aplicaciones web	Aplicaciones Web	30	5,850.00	351,000.00
Firewall de base de datos	Base de datos	60	29,676.00	3,561,120.00
			PRECIOS TOTALES ANTES DE IVA	3,912,120.00
			IVA	625,939.20
			PRECIOS TOTALES INCLUYENDO IVA	4,538,059.20

Servicio Administrado de Seguridad Bajo Demanda	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Análisis de código estático y dinámico	Evento	2	44,792.00	179,168.00
			PRECIOS TOTALES ANTES DE IVA	179,168.00
			IVA	28,666.88
			PRECIOS TOTALES INCLUYENDO IVA	207,834.88

Servicio Administrado de Seguridad Bajo Demanda	UNIDAD DE MEDIDA	CANTIDAD MÁXIMA MENSUAL (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO MÁXIMOS (AxBx2)
Protección del Servicio de Verificación de la Credencial para Votar	Hardware (Equipos)	1	259,090.00	518,180.00
			PRECIOS TOTALES ANTES DE IVA	518,180.00
			IVA	82,908.80
			PRECIOS TOTALES INCLUYENDO IVA	601,088.80

SERVICIOS	UNIDAD DE MEDIDA	UNIDADES TOTALES (A)	PRECIO UNITARIO MENSUAL (B)	PRECIO TOTAL (AxB)
Servicio de Gestión de Seguridad de la Información	MES DE SERVICIO	2	402,977.00	805,954.00
PRECIOS TOTALES ANTES DE IVA				805,954.00
IVA				128,952.64
PRECIOS TOTALES INCLUYENDO IVA				934,906.64

RESUMEN DE LA PROPUESTA ECONOMICA	
SERVICIO	SUMA DE LOS PRECIOS TOTALES DE TODAS LAS TABLAS
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DE SEGURIDAD INFORMÁTICA	12,604,506.00
PRECIOS TOTALES ANTES DE IVA	12,604,506.00
IVA	2,016,720.96
PRECIOS TOTALES INCLUYENDO IVA	14,621,226.96

Monto en Letra Precio mínimo: N/A
Monto en Letra Precio máximo: $12,604,506.00 M.N. (Doce millones seiscientos cuatro mil quinientos seis pesos 00/100 MXN), antes de I.V.A.
Datos de contacto:
Correo: infolicitaciones@iqsec.com.mx
Número Telefónico: 55-4163-1700
Vigencia de Cotización: 60 días naturales

ATENTAMENTE

Yolanda Saldaña Tavera
Representante Legal
IQSEC, S.A. DE C.V.