CONTRATO **PARA LA PRESTACIÓN DEL SERVICIO INTEGRAL DE FORTALECIMIENTO EN LA GESTIÓN, ADMINISTRACIÓN Y CONTROL DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES**, QUE CELEBRAN, POR UNA PARTE, EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES REPRESENTADO POR LA C. ERIKA HELENA PSIHAS VALDÉS, EN SU CARÁCTER DE APODERADA LEGAL, EN ADELANTE **"EL INSTITUTO FONACOT"** Y, POR LA OTRA, LA EMPRESA DENOMINADA IQSEC, S.A. DE C.V., EN LO SUCESIVO **"EL PRESTADOR"**, REPRESENTADA POR EL C. ALLAN MORGAN VELASCO, EN SU CARÁCTER DE APODERADO 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 un organismo público descentralizado de interés social, con personalidad jurídica y patrimonio propio, así como con autosuficiencia presupuestal y sectorizado en la Secretaría del Trabajo y Previsión Social, 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.

I.2 Conforme a lo dispuesto en el poder que le fue conferido mediante escritura pública número 223,288 de fecha 1°. de abril del 2022, ante la fe del Mtro. Eutiquio López Hernández, Notario Público número 35 de la Ciudad de México; documento que quedó debidamente inscrito en el Registro Público de Organismos Descentralizados, bajo el folio número 82-7-13042022-201316 el día 13 de abril de 2022; de conformidad con lo establecido por los artículos 24 y 25 de la Ley Federal de las Entidades Paraestatales y 40, 41, 45 y 46 de su Reglamento, la **C. Erika Helena Psihas Valdés**, Directora de Recursos Materiales y Servicios Generales, Encargada y Responsable de los Asuntos de la Subdirección General de Administración con fundamento en el artículo 79 del Estatuto Orgánico de **"EL INSTITUTO FONACOT"** y Apoderada Legal, con R.F.C. PIVE700829LI7, es la persona servidora pública que tiene conferidas las facultades legales para celebrar el presente contrato, quien podrá ser sustituido en cualquier momento en su cargo o funciones, sin que ello implique la necesidad de elaborar convenio modificatorio.

I.3 De conformidad con el Estatuto Orgánico del Instituto del Fondo Nacional para el Consumo de los Trabajadores de fecha 15 de julio del 2022, suscribe el presente instrumento el **C. Horacio Sánchez Tinoco**, en su calidad de Subdirector General de Tecnologías de la Información y Comunicación con R.F.C. SATH771010TB3, facultado para administrar el cumplimiento de las obligaciones que deriven del objeto del presente contrato, quien podrá ser sustituido en cualquier momento en su cargo o funciones, bastando para tales efectos un comunicado por escrito y firmado por el servidor público facultado para ello, dirigido al representante de **"EL PRESTADOR"** para los efectos del presente contrato, encargados del cumplimiento de las obligaciones contraídas en el presente instrumento jurídico.

I.4 De conformidad con el apartado VI, numeral 14 inciso b) de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del Instituto FONACOT, suscribe el presente instrumento la **C. Erika Helena Psihas Valdés,** Directora de Recursos Materiales y Servicios Generales, R.F.C PIVE700829LI7, facultada para actuar en calidad de área contratante.

I.5 La adjudicación del presente contrato se realizó mediante el procedimiento de **Adjudicación Directa por excepción a la Licitación Pública**, realizado al amparo de lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos y en los artículos **25**, **26 fracción III, 40, y 41 fracción III** de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"LAASSP"**, y los correlativos de su Reglamento contando con el dictamen favorable por parte del Comité de Adquisiciones, Arrendamientos y Servicios del Instituto FONACOT, en su Quinta Sesión Extraordinaria, celebrada el 18 de agosto de 2022.

I.6 **"EL INSTITUTO FONACOT"** cuenta con recursos suficientes y con autorización para ejercerlos en el cumplimiento de sus obligaciones derivadas del presente contrato, en la partida presupuestal **33304,** denominada **Servicio de Mantenimiento de Aplicaciones Informáticas** con oficio número **SGA-**

342-2022, de fecha **11 de julio de 2022,** emitido por la Dirección de Recursos Materiales y Servicios Generales, Encargada y Responsable de los Asuntos de la Subdirección General de Administración.

I.7 Para efectos fiscales las Autoridades Hacendarias le han asignado el Registro Federal de Contribuyentes **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 PRESTADOR"** declara que:

Eliminado OCR o NÚMERO IDENTIFICADOR. Ubicado en el octavo renglón del sexto párrafo. **Fundamento legal**: Artículo 116 de la Ley General de Transparencia y Acceso a la Información Pública y 113 fracción I de la Ley Federal de Transparencia y Acceso a Información Pública, en relación con el artículo 3 fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el Lineamiento Trigésimo Octavo fracción I de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información. **Motivación:** El número de credencial de elector denominado Reconocimiento Óptico de Caracteres (OCR), contiene el número de la sección electoral en donde vota el ciudadano titular de dicho documento, por lo que constituye un dato personal en razón de que revela información concerniente a una persona física identificada o identificable.

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, Notario Público número 140 de la Ciudad de México, e inscrita en el Registro Público de Comercio de la Ciudad de México, en el folio mercantil número 371652.

II.2 El **C. Allan Morgan Velasco**, en su carácter de apoderado legal, cuenta con poder suficiente para suscribir el presente contrato, de conformidad con lo establecido en la escritura pública número 116,940 de fecha 28 de marzo de 2022, otorgado ante la fe del Lic. Jorge Alfredo Domínguez Martínez, Notario Público número 140 de la Ciudad de México, por el cual se le confirió poder general para actos de administración, con todas las facultades administrativas, en los términos del segundo párrafo del artículo 2554 del Código Civil para el Distrito Federal y sus correlativos, declarando bajo protesta de decir verdad, que a la fecha, dicho poder no le ha sido modificado ni revocado en forma alguna, asimismo, se identifica con su credencial para votar [redacted] expedida por el Instituto Nacional Electoral, con vigencia al año 2030.

II.3 Ha considerado todos y cada uno de los factores que intervienen en el presente contrato, manifestando reunir las condiciones técnicas, jurídicas y económicas, así como la organización y elementos necesarios para su cumplimiento.

II.4 Bajo protesta de decir verdad, manifiesta que ni él ni ninguno de los socios o accionistas desempeñan un empleo, cargo o comisión en el servicio público, ni se encuentran inhabilitados para ello, o en su caso que, a pesar de desempeñarlo, con la formalización del presente contrato no se actualiza un conflicto de interés, en términos del artículo 49, fracción IX de la Ley General de Responsabilidades Administrativas lo cual se constató por el Órgano Interno de Control en **"EL INSTITUTO FONACOT"**, en concordancia con los artículos 50, fracción II de la **"LAASSP"** y 88, fracción I de su Reglamento; así como que **"EL PRESTADOR"** no se encuentra en alguno de los supuestos del artículo 50 y penúltimo y antepenúltimo párrafos del artículo 60 de la **"LAASSP"**.

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

II.6 Cuenta con su Registro Federal de Contribuyentes IQS0708233C9**.**

II.7 Bajo protesta de decir verdad, manifiesta estar al corriente en los pagos que se derivan de sus obligaciones fiscales, en específico de las previstas en el artículo 32-D del Código Fiscal Federal vigente, así como de sus obligaciones fiscales en materia de seguridad social, ante el Instituto del Fondo Nacional de la Vivienda para los Trabajadores y el Instituto Mexicano del Seguro Social; lo que acredita con las Opiniones de Cumplimiento de Obligaciones Fiscales y en materia de Seguridad Social en sentido positivo, emitidas por el SAT e IMSS respectivamente, así como con la Constancia de Situación Fiscal en materia de Aportaciones Patronales y Entero de Descuentos, sin adeudo emitida por el INFONAVIT, las cuales se encuentran vigentes y obran en el expediente respectivo.

II.8 Señala como su domicilio para todos los efectos legales el ubicado en Avenida Patriotismo número 399, Colonia San Pedro de los Pinos, Demarcación Territorial Benito Juárez, Código Postal 03800, Ciudad de México.

III. De "LAS PARTES":

III.1 Que es su voluntad celebrar el presente contrato y sujetarse a sus términos y condiciones, para lo cual se reconocen ampliamente las facultades y capacidades necesarias, mismas que no les han sido revocadas o limitadas en forma alguna, por lo que de común acuerdo se obligan de conformidad con las siguientes:

CLÁUSULAS

PRIMERA. OBJETO DEL CONTRATO.

"EL PRESTADOR" acepta y se obliga a proporcionar a **"EL INSTITUTO FONACOT"** la prestación del **Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones**, al amparo del procedimiento de contratación señalado en el punto I.5 de las declaraciones de este instrumento jurídico y de conformidad con la descripción, características, plazo, entregables y condiciones que se detallan en su Anexo Técnico, que como Anexo I se agrega al presente contrato, el cual una vez rubricado por las "**PARTES**", formaran parte integrante del mismo.

SEGUNDA. DE LOS MONTOS Y PRECIOS

Los precios unitarios del presente contrato se detallan en la Cotización, que como Anexo II se agrega al presente contrato, el cual una vez rubricado por las PARTES, formará parte integrante del mismo.

El monto total del mismo es por la cantidad de $12,408,608.52 (Doce millones cuatrocientos ocho mil seiscientos ocho pesos, 52/100 M.N.) cantidad antes de IVA.

Los precios unitarios son considerados fijos y en moneda nacional (pesos mexicanos) hasta que concluya la relación contractual que se formaliza, incluyendo **"EL PRESTADOR"** todos los conceptos y costos involucrados en la prestación del, **Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones** por lo que **"EL PRESTADOR"** no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.

TERCERA. FORMA Y LUGAR DE PAGO (ODCS y RICG)

"EL INSTITUTO FONACOT" se obliga a pagar a **"EL PRESTADOR"** la cantidad señalada en la cláusula segunda de este instrumento jurídico, en moneda nacional, en un plazo máximo de 20 días naturales siguientes, a partir de la fecha en que sea entregado y aceptado el Comprobante Fiscal Digital por Internet (CFDI) o factura electrónica por **"EL INSTITUTO FONACOT"**, con la aprobación (firma) del Administrador del presente contrato mencionado en la Declaración I.3.

El pago se realizará en pagos mensuales o de acuerdo con los servicios devengados debidamente soportado y acompañado con los entregables que apliquen del Anexo Técnico.

El cómputo del plazo para realizar el pago se contabilizará a partir del día hábil siguiente de la recepción del CFDI o factura electrónica, esto considerando que no existan aclaraciones al importe, para lo cual es necesario que el CFDI o factura electrónica que se presente reúna los requisitos fiscales que establece la legislación en la materia y los precios unitarios; asimismo, deberá acompañarse con la documentación completa y debidamente requisitada.

De conformidad con el artículo 90 del Reglamento de la **"LAASSP"**, en caso de que el CFDI o factura electrónica entregado presenten errores, el Administrador del presente contrato mencionado en la Declaración I.3, dentro de los 3 (tres) días hábiles siguientes de su recepción, indicará a **"EL PRESTADOR"** las deficiencias que deberá corregir; por lo que, el procedimiento de pago reiniciará en el momento en

que **"EL PRESTADOR"** presente el CFDI o factura electrónica corregido.

El tiempo que **"EL PRESTADOR"** utilice para la corrección de la documentación entregada, no se computará para efectos de pago, de acuerdo con lo establecido en el artículo 51 de la **"LAASSP"**.

Los CFDI's (facturas) deberán contar 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 12 "Características Técnicas del Servicio"**, mismos que deberán de ser entregados en las oficinas centrales del Instituto FONACOT, ubicadas en Avenida Insurgentes Sur No. 452, 5to. Piso, Colonia Roma Sur, Código Postal 06760, Demarcación Territorial Cuauhtémoc, Ciudad de México, , en la Subdirección General de Tecnologías de la Información y Comunicación, así mismo deberá ser enviada al correo electrónico horacio.sanchez@fonacot.gob.mx en un horario de labores de las 9:00 a las 18:00 horas de lunes a viernes.

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 IVA cuando aplique.

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

Para efectos de trámite de pago, **"EL PRESTADOR"** deberá ser titular de una cuenta de cheques vigente y para tal efecto proporciona las CLABE [redacted] de la institución bancaria **BBVA BANCOMER**, a nombre de IQSEC, S.A. de C.V., en la que se efectuará la transferencia electrónica de pago, debiendo anexar:

1. Constancia de la institución financiera sobre la existencia de la cuenta de cheques abierta a nombre del beneficiario que incluya:
   - Nombre del beneficiario (conforme al timbre fiscal);
   - Registro Federal de Contribuyentes;
   - Domicilio fiscal: calle, N° exterior, N° interior, colonia, código postal, alcaldía y entidad federativa;
   - Nombre(s) del(los) banco(s); y
   - Número de la cuenta con once dígitos, así como la Clave Bancaria Estandarizada (CLABE) con 18 dígitos, que permita realizar transferencias electrónicas de fondo, a través del Sistema de Pago.
2. Copia de estado de cuenta reciente, con no más de dos meses de antigüedad.

El pago de los servicios recibidos, quedará condicionado proporcionalmente al pago que **"EL PRESTADOR"** deba efectuar por concepto de penas convencionales.

El pago será efectuado mediante transferencia bancaria a la cuenta que **"EL PRESTADOR"** proporcione.

Para el caso de que se presenten pagos en exceso, se estará a lo dispuesto por el artículo 51 párrafo tercero, de la **"LAASSP"**.

Eliminado DATOS BANCARIOS (No. de cuenta y CLABE). Ubicados en el octavo renglón del segundo párrafo. **Fundamento Legal:** Artículo 116 de la Ley General de Transparencia y Acceso a la Información Pública y 113 fracción I de la Ley Federal de Transparencia y Acceso a Información Pública, en relación con el artículo 3 fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el Lineamiento Trigésimo Octavo fracción I de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información y criterio 10/17 emitido por el INAI. **Motivación:** El número de cuenta bancaria y/o CLABE interbancaria de personas físicas o morales privadas es información confidencial, al tratarse de un conjunto de caracteres numéricos utilizados por los grupos financieros para identificar las cuentas de sus clientes, a través de los cuales se puede acceder a información relacionada con su patrimonio y realizar diversas transacciones.

CUARTA. VIGENCIA

El contrato comprenderá una vigencia considerada a partir del 20 de agosto del 2022 y hasta el 31 de diciembre del 2022 **"LAS PARTES"** están de acuerdo en que por necesidades de **"EL INSTITUTO FONACOT"** podrá ampliarse, la prestación del servicio objeto del presente contrato, de conformidad con el artículo 52 de la **"LAASSP"**, siempre y cuando las modificaciones no rebasen en su conjunto el 20% (veinte por ciento) del monto o cantidad de los conceptos y volúmenes establecidos originalmente. Lo anterior, se formalizará mediante la celebración de un Convenio Modificatorio del Contrato Principal. Asimismo, con fundamento en el artículo 91 del Reglamento de la **"LAASSP"**, **"EL PRESTADOR"** deberá entregar las modificaciones respectivas de las garantías, señaladas en la **CLÁUSULA SÉPTIMA** de este contrato.

Por caso fortuito o de fuerza mayor, o por causas atribuibles a **"EL INSTITUTO FONACOT"**, se podrá modificar el presente instrumento jurídico, la fecha o el plazo para la prestación de los servicios. En dicho supuesto, se deberá formalizar el convenio modificatorio respectivo, no procediendo la aplicación de penas convencionales por atraso. Tratándose de causas imputables a **"EL INSTITUTO FONACOT"**, no se requerirá de la solicitud de **"EL PRESTADOR"**.

QUINTA. GARANTÍA DE CUMPLIMIENTO DEL CONTRATO.

Conforme a los artículos 48 fracción II, y 49 fracción II, de la **"LAASSP"**, 87 de su Reglamento; 166 de la Ley de Instituciones de Seguros y de Fianzas, las Disposiciones Generales a que se sujetarán las garantías otorgadas a favor del Gobierno Federal para el cumplimiento de obligaciones distintas de las fiscales que constituyan las Dependencias y Entidades en los actos y contratos que celebren, publicadas en el DOF el 08 de septiembre de 2015, **"EL PRESTADOR"** se obliga a constituir una garantía divisible por el importe del 10% (diez por ciento) del monto máximo por erogar, a favor del Instituto del Fondo Nacional para el Consumo de los Trabajadores, la cual deberá ser entregada dentro de los 10 (diez) días naturales siguientes a la fecha de firma del presente contrato.

La fianza deberá entregarse en la Dirección de Recursos Materiales y Servicios Generales del Instituto FONACOT cita en Avenida Insurgentes Sur No. 452, piso 1, Colonia Roma Sur, Demarcación Territorial Cuauhtémoc, Código Postal 06760, Ciudad de México, en los tiempos mencionados en el párrafo anterior.

Si las disposiciones jurídicas aplicables lo permitan, la entrega de la garantía de cumplimiento se realice de manera electrónica.

- Expedirse a favor del Instituto del Fondo Nacional para el Consumo de los Trabajadores con domicilio en Avenida Insurgentes Sur No. 452, Colonia Roma Sur, Demarcación Territorial Cuauhtémoc, Código Postal 06760, Ciudad de México;
- La indicación del importe total garantizado con número y letra;
- La referencia de que la fianza se otorga atendiendo a todas las estipulaciones contenidas en el contrato y el anexo respectivo, así como la cotización y el requerimiento asociado a ésta;
- La información correspondiente al número de contrato, su fecha de firma, así como la especificación de las obligaciones garantizadas;
- El señalamiento de la denominación o nombre de **"EL PRESTADOR"** y de la institución afianzadora, así como sus domicilios correspondientes;
- La condición de que la vigencia de la fianza deberá quedar abierta para permitir que cumpla con su objetivo, y continuará vigente durante la sustanciación de todos los recursos legales o juicios que se interpongan hasta que se dicte resolución definitiva por la autoridad competente, de forma tal que no podrá establecerse o estipularse plazo alguno que limite su vigencia, lo cual no debe confundirse con el plazo para el cumplimiento de las obligaciones previstas en el contrato y actos administrativos garantizados;
- La indicación de que la fianza se hará efectiva conforme al procedimiento dispuesto en el artículo 282 de la Ley de Instituciones de Seguros y de Fianzas, el cual será aplicable también para el cobro de los intereses que en su caso se generen en los términos previstos en el artículo 283 del propio ordenamiento;
- La indicación de que la cancelación de la póliza de fianza procederá una vez que **"EL INSTITUTO FONACOT"** otorgue el documento en el que se señale la extinción de derechos y obligaciones,

previo otorgamiento del finiquito correspondiente, o en caso de existir saldos a cargo de **"EL PRESTADOR"**, la liquidación debida;

- Para acreditar a la institución afianzadora el incumplimiento de la obligación garantizada, tendrá que cumplirse con los requisitos establecidos en las Disposiciones Generales a que se sujetarán las garantías otorgadas a favor del Gobierno Federal para el cumplimiento de obligaciones distintas de las fiscales que constituyan las dependencias y entidades en los actos y contratos que celebren, publicadas en el Diario Oficial de la Federación el 08 de septiembre de 2015; y
- El momento de inicio de la fianza y, en su caso, su vigencia.

Considerando los requisitos anteriores, dentro de la fianza, se deberán incluir las declaraciones siguientes en forma expresa:

- "Esta garantía estará vigente durante la sustanciación de todos los recursos legales o juicios que se interpongan hasta que se pronuncie resolución definitiva por autoridad competente, de forma tal que su vigencia no podrá acotarse en razón del plazo de ejecución del contrato.
- "La institución de fianzas acepta expresamente someterse al procedimiento de ejecución establecido en el artículo 282 de la Ley de Instituciones de Seguros y de Fianzas, para la efectividad de la presente garantía, procedimiento al que también se sujetará para el caso del cobro de intereses que prevé el artículo 283 del mismo ordenamiento legal, por pago extemporáneo del importe de la póliza de fianza requerida.";
- "La cancelación de la fianza no procederá sino en virtud de manifestación previa de manera expresa y por escrito de **"EL INSTITUTO FONACOT"**."; y
- "La afianzadora acepta expresamente tener garantizado el contrato a que esta póliza se refiere, aún en el caso de que se otorgue prórroga o espera al deudor principal o fiado por parte de **"EL INSTITUTO FONACOT"** para el cumplimiento total de las obligaciones que se garantizaran, por lo que la afianzadora renuncia expresamente al derecho que le otorga el artículo 179 de la Ley de Instituciones de Seguros y de Fianzas."

De no cumplir con dicha entrega, **"EL INSTITUTO FONACOT"** podrá rescindir el contrato y remitir el asunto al Órgano Interno de Control para que determine si se aplican las sanciones estipuladas en el artículo **60** fracción **III** de la **"LAASSP"**.

La garantía de cumplimiento de ninguna manera será considerada como una limitación de la responsabilidad de **"EL PRESTADOR"**, derivada de sus obligaciones y garantías estipuladas en el presente instrumento jurídico, y de ninguna manera impedirá que **"EL INSTITUTO FONACOT"** reclame la indemnización o el reembolso 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 PRESTADOR"** se obliga a entregar a **"EL INSTITUTO FONACOT"** dentro de los 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.

"EL PRESTADOR" acepta expresamente que la garantía expedida para garantizar el cumplimiento se hará efectiva independientemente de que se interponga cualquier otro tipo de recurso ante instancias del orden administrativo o judicial, así como que permanecerá vigente durante la substanciación de los juicios o recursos legales que se interponga con relación a dicho contrato, hasta que sea pronunciada resolución definitiva que cause ejecutoria por la autoridad competente.

El trámite de liberación de garantía, se realizará inmediato a que se extienda la constancia de cumplimiento de obligaciones contractuales por parte de **"EL INSTITUTO FONACOT"**, de conformidad con lo dispuesto por el artículo 81, fracción VIII del Reglamento de la **"LAASSP"**.

Considerando que la entrega de los servicios, cuando aplique se haya previsto un plazo menor a diez días naturales, se exceptúa el cumplimiento de la garantía, de conformidad con lo establecido en el artículo 48 último párrafo de la **"LAASSP",** en concordancia con lo señalado en el tercer párrafo del artículo 86 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Para este caso, el monto máximo de las penas convencionales por atraso que se puede aplicar, será del veinte por ciento del monto de los servicios entregados fuera de la fecha convenida, de conformidad con lo establecido en el tercer párrafo del artículo 96 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

SEXTA. RESPONSABILIDAD CIVIL.

"EL PRESTADOR" se obliga a proporcionar al administrador del contrato una póliza expedida por institución autorizada por las Leyes Mexicanas a favor del Instituto del Fondo Nacional para el Consumo de los Trabajadores, por un importe de $3,000,000.00 (Tres millones de pesos 00/100 M.N.) que garantice la protección de daños y perjuicios que pudieran presentarse como resultado de las actividades propias de **"EL PRESTADOR"** por la ejecución de los servicios derivados del presente contrato, y de conformidad al Anexo Técnico, que como Anexo I se agrega al presente Contrato, el cual una vez rubricado por las partes formara parte integrante del mismo, .

SÉPTIMA. OBLIGACIONES DE "EL PRESTADOR"

a) Prestar los servicios en las fechas o plazos y lugares específicos conforme a lo requerido en el presente contrato y anexos respectivos.
b) Cumplir con las especificaciones técnicas y de calidad y demás condiciones establecidas en el contrato y su respectivo anexo, así como la cotización y el requerimiento asociado a ésta;
c) Asumir su responsabilidad ante cualquier situación que pudiera generarse con motivo del presente contrato.
d) No difundir a terceros sin autorización expresa de **"EL INSTITUTO FONACOT"** la información que le sea proporcionada, inclusive después de la rescisión o terminación del presente instrumento, sin perjuicio de las sanciones administrativas, civiles y penales a que haya lugar.
e) Proporcionar la información que le sea requerida por parte de la Secretaría de la Función Pública y el Órgano Interno de Control, de conformidad con el artículo 107 del Reglamento de la **"LAASSP"**.

OCTAVA. OBLIGACIONES DE "EL INSTITUTO FONACOT"

a) Otorgar todas las facilidades necesarias, a efecto de que **"EL PRESTADOR"** lleve a cabo en los términos convenidos.
b) Sufragar el pago correspondiente en tiempo y forma, por la prestación de los servicios.
c) Extender a **"EL PRESTADOR",** en caso de que lo requiera, por conducto del Administrador del Contrato, la constancia de cumplimiento de obligaciones contractuales inmediatamente que se cumplan éstas a satisfacción expresa de dicho servidor público para que se dé trámite a la cancelación de la garantía de cumplimiento del presente contrato.

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

La prestación de los servicios, será conforme a los plazos, condiciones y entregables establecidos por **"EL INSTITUTO FONACOT"** en el Anexo I del presente contrato.

La prestación de los servicios, se realizará en los domicilios señalados en el Anexo I del presente contrato y en las fechas establecidas en el mismo.

Señalar si existirá el otorgamiento de prórrogas para el cumplimiento de las obligaciones contractuales y los requisitos que deberán observarse, así como el servidor público facultado para el otorgamiento de la misma.

DÉCIMA. LICENCIAS

"EL PRESTADOR" será responsable de proporcionar el licenciamiento necesario para que el personal autorizado del área técnica de **"EL INSTITUTO FONACOT"** acceda a las consolas de las tecnologías inherentes al contrato.

Es responsabilidad de **"EL PRESTADOR"** mantener el licenciamiento vigente y efectuar las actualizaciones hacia las nuevas versiones disponibles e incorporando nuevas funcionalidades de las mismas durante toda la vigencia del contrato, sin costo adicional para **"EL INSTITUTO FONACOT".**

DÉCIMA PRIMERA. CALIDAD

"EL PRESTADOR" deberá contar con la infraestructura necesaria, personal técnico especializado en el ramo, herramientas, técnicas y equipos adecuados para proporcionar la prestación de los servicios requeridos, a fin de garantizar que el objeto de este contrato sea proporcionado con la calidad, oportunidad y eficiencia requerida para tal efecto, comprometiéndose a realizarlo a satisfacción de **"EL INSTITUTO FONACOT"** y con estricto apego a lo establecido en las cláusulas del presente instrumento jurídico y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta.

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

DÉCIMA SEGUNDA. RESPONSABILIDAD

"EL PRESTADOR" se obliga a responder por su cuenta y riesgo de los daños y/o perjuicios que por inobservancia o negligencia de su parte lleguen a causar a **"EL INSTITUTO FONACOT"**, con motivo de las obligaciones pactadas, o bien por los defectos o vicios ocultos en los servicios, de conformidad con lo establecido en el artículo 53 de la **"LAASSP"**.

DÉCIMA TERCERA. 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 PRESTADOR"**, mismos que no serán repercutidos a **"EL INSTITUTO FONACOT"**.

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

DÉCIMA CUARTA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES

"EL PRESTADOR" 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"** deslindando a ésta de toda responsabilidad.

DÉCIMA QUINTA. DERECHOS DE AUTOR, PATENTES Y/O MARCAS

"EL PRESTADOR" asume la responsabilidad total en caso de que, la prestación de los servicios, objeto del presente contrato, infrinja patentes, marcas o viole otros registros de derechos de propiedad industrial a nivel nacional e internacional, 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.

En tal virtud, **"EL PRESTADOR"** manifiesta en este acto bajo protesta de decir verdad, no encontrarse en ninguno de los supuestos de infracción administrativa y/o delito establecidos en la Ley Federal del Derecho de Autor ni en la Ley de la Propiedad Industrial.

En caso de que sobreviniera alguna reclamación en contra de **"EL INSTITUTO FONACOT"**, por cualquiera de las causas antes mencionadas, la única obligación de ésta será la de dar aviso en el domicilio previsto en el apartado de Declaraciones de este instrumento a **"EL PRESTADOR"**, para que éste, utilizando los medios correspondientes al caso, garantice salvaguardar a **"EL INSTITUTO FONACOT"** de cualquier controversia, liberándole de toda responsabilidad de carácter civil, penal, mercantil, fiscal o de cualquier otra índole.

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

DÉCIMA SEXTA. CONFIDENCIALIDAD

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

La información contenida en el presente contrato es pública, de conformidad con lo dispuesto en los artículos 70 fracción XXVIII de la Ley General de Transparencia y Acceso a la Información Pública y 68 de la Ley Federal de Transparencia y Acceso a la Información Pública; sin embargo la información que proporcione **"EL INSTITUTO FONACOT"** a **"EL PRESTADOR"** para el cumplimiento del objeto materia del mismo, será considerada como confidencial en términos de los artículos 116 y 113, respectivamente, de los citados ordenamientos jurídicos, por lo que **"EL PRESTADOR"** se compromete a recibir, proteger y guardar la información confidencial proporcionada por **"EL INSTITUTO FONACOT"** con el mismo empeño y cuidado que tiene respecto de su propia información confidencial, así como hacer cumplir a todos y cada uno de los usuarios autorizados a los que les entregue o permita acceso a la información confidencial, en los términos de este instrumento.

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

Cuando de las causas descritas en las cláusulas de RESCISIÓN y TERMINACIÓN ANTICIPADA, del presente contrato, concluya la vigencia del mismo, subsistirá la obligación de confidencialidad sobre los servicios establecidos en este instrumento legal.

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

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

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

Asimismo, **"EL PRESTADOR"** no podrá, con motivo de la prestación de los servicios que realice a **"EL INSTITUTO FONACOT"**, utilizar la información a que tenga acceso, para asesorar, patrocinar o constituirse en consultor de cualquier persona que tenga relaciones directas o indirectas con el objeto de las actividades que lleve a cabo.

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

"EL INSTITUTO FONACOT" designa como responsable de administrar y vigilar el cumplimiento del presente contrato al C. Horacio Sánchez Tinoco en su calidad de Subdirector General de Tecnologías de

la información y Comunicación con- el objeto de verificar el óptimo cumplimiento del mismo, por lo que indicará a **"EL PRESTADOR"** las observaciones que se estimen pertinentes, quedando éste obligado a corregir las anomalías que le sean indicadas, así como deficiencias en la entrega de los servicios o de su personal.

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

Los servicios serán recibidos previa revisión del administrador del contrato.

En tal virtud, **"EL PRESTADOR"** manifiesta expresamente su conformidad de que hasta en tanto no se cumpla de conformidad con lo establecido en el párrafo anterior, los servicios no se tendrán por aceptados por parte de **"EL INSTITUTO FONACOT"**.

DÉCIMA OCTAVA. DEDUCCIONES

En caso de que **"EL PRESTADOR"** incurra en incumplimiento de cualquiera de sus obligaciones contractuales de forma parcial o deficiente a lo estipulado en las cláusulas del presente contrato y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta, **"EL INSTITUTO FONACOT"** por conducto del administrador del contrato aplicará una deducción de acuerdo a lo siguiente:

DEDUCTIVAS		
No.	**Descripción**	**Monto**
1	Incumplimiento parcial o entrega mal realizada o incompleta en los niveles de servicio establecidos en el numeral **21. NIVELES DE SERVICIO (SLA´s).**	3% del monto total mensual del mes en cuestión, por incumplimiento parcial o entrega mal realizada o incompleta a los niveles de servicio.
2	Incumplimiento en la entrega total de cada uno de los servicios, ya sea por mala realización o entrega incompleta, de cualquiera de los servicios plasmados en el numeral **5. DESCRIPCIÓN GENERAL DEL SERVICIO**.	3% del monto total mensual del mes en cuestión, por incumplimiento en la entrega total de cada uno de los servicios, ya sea por mala realización o entrega incompleta, de cualquiera de los servicios plasmados, por más de 1 hora.
3	Incumplimiento en el tiempo de asignación o reemplazo de los recursos humanos, establecidos en el numeral **13. ADMINISTRACIÓN DE LOS SERVICIOS**.	1% del monto total mensual del mes en cuestión, por día natural por incumplimiento parcial o fuera de los tiempos establecidos para el reemplazo de los recursos humanos.
4	Incumplimiento parcial o entrega mal realizada o incompleta por cada uno de los entregables mensuales, establecidos en el numeral **22. ENTREGABLES**.	3% del monto total mensual del mes en cuestión, por día natural por incumplimiento parcial o entrega mal realizada o incompleta de cada uno de los entregables mensuales.

Los montos a deducir se aplicarán en el CFDI o factura electrónica que **"EL PRESTADOR"** presente para su cobro, en el pago que se encuentre en trámite o bien en el siguiente pago.

Para el pago de las deductivas, el área requirente informará por escrito a **"EL PRESTADOR"**- el cálculo de la deductiva a la que se hizo acreedor, por el incumplimiento parcial o deficiente en que haya incurrido **"EL PRESTADOR"**.

En caso de no existir pagos pendientes, la deducción se aplicará sobre la garantía de cumplimiento del contrato siempre y cuando **"EL PRESTADOR"** no realice el pago de la misma.

Lo anterior, en el entendido de que se cumpla con el objeto de este contrato de forma inmediata, conforme a lo acordado. En caso contrario, **"EL INSTITUTO FONACOT"** podrá iniciar en cualquier momento posterior al incumplimiento, el procedimiento de rescisión del contrato, considerando la gravedad del

incumplimiento y los daños y perjuicios que el mismo pudiera ocasionar a los intereses del Estado, representados por **"EL INSTITUTO FONACOT"**.

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

La notificación y cálculo de las deducciones correspondientes las realizará el administrador del contrato de **"EL INSTITUTO FONACOT"**.

Cuando el monto total de aplicación de deducciones alcance el 10% (diez por ciento) del monto total del contrato, se iniciará el procedimiento de rescisión.

DÉCIMA NOVENA. PENAS CONVENCIONALES

En caso de que **"EL PRESTADOR"** presente atraso en el cumplimiento de cualquiera de sus obligaciones pactadas para la prestación de los servicios, objeto del presente contrato, **"EL INSTITUTO FONACOT"**, por conducto de la Dirección de Recursos Materiales y Servicios Generales aplicará una pena convencional conforme a lo siguiente:

PENAS CONVENCIONALES		
No.	Descripción	Monto
1	Minuta de la Reunión de Kick Off de este con el numeral 22. ENTREGABLES del Anexo Técnico.	1% del monto total mensual del mes en cuestión, por día natural de atraso en la entrega de la Minuta de la Reunión de Kick Off, debidamente firmada por los asistentes por parte de **"EL PRESTADOR"** la cual deberá entregarse a más tardar a los cinco días hábiles de haberse llevado a cabo la referida reunión.
2	Atraso en la entrega del Plan de Trabajo General de conformidad con el numeral 22. ENTREGABLES del Anexo Técnico.	1% del monto total mensual del mes en cuestión, por día natural de atraso en la entrega del Plan de Trabajo General, el cual deberá entregarse a más tardar a los cinco días hábiles después de firmado el Contrato.
3	Atraso en la entrega del Plan de Trabajo Detallado por Servicio a Implementar, de acuerdo con las necesidades del servicio integral de conformidad con el numeral 22 ENTREGABLES del Anexo Técnico.	1% del monto total mensual del mes en cuestión, por día natural de atraso en la entrega de los Planes de Trabajo a Detalle para la implementación de cada servicio, dichos planes detallados deberán entregarse a más tardar a los diez días hábiles después de entregado el Plan de Trabajo General.
4	Memoria Técnica de cada Servicio Implementado de conformidad con el numeral 22 ENTREGABLES del Anexo Técnico.	1% del monto total mensual del mes en cuestión, por día natural de atraso en la entrega de la Memoria Técnica, la cual deberá entregarse a más tardar a los cinco días de concluido la implementación respectiva del servicio correspondiente.
5	Atraso en los tiempos establecidos en la implementación de los servicios objetos de conformidad con el numeral 22 ENTREGABLES del Anexo Técnico.	3% del monto total mensual del mes en cuestión, por día natural de atraso en la implementación de cada uno de los servicios objeto del presente, de acuerdo a su plan de trabajo detallado correspondiente.

Por lo anterior, el pago de la prestación de los servicios quedará condicionado, proporcionalmente, al pago que **"EL PRESTADOR"** deba efectuar por concepto de penas convencionales por atraso, en el entendido de que, si el contrato es rescindido en términos de lo previsto en la CLÁUSULA DE RESCISIÓN, no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento del contrato.

Para efectuar este pago, **"EL PRESTADOR"** contará con un plazo que no excederá de 5 (cinco) días hábiles contados a partir de la fecha de recepción de la notificación; a través de nota de crédito.

Cuando la suma de las penas convencionales exceda el monto total de la garantía de cumplimiento del presente contrato, se iniciará el procedimiento de rescisión del mismo, en los términos del artículo 54 de la **"LAASSP"**.

Independientemente de la aplicación de la pena convencional a que hace referencia el párrafo que antecede, se aplicarán además cualquiera otra que la **"LAASSP"** establezca.

Esta pena convencional no descarta que **"EL INSTITUTO FONACOT"** en cualquier momento posterior al incumplimiento determine procedente la rescisión del contrato, considerando la gravedad de los daños y perjuicios que el mismo pudiera ocasionar a los intereses de **"EL INSTITUTO FONACOT"**.

En caso que sea necesario llevar a cabo la rescisión administrativa del contrato, la aplicación de la garantía de cumplimiento será por el monto total de las obligaciones garantizadas.

La penalización tendrá como objeto resarcir los daños y perjuicios ocasionados a **"EL INSTITUTO FONACOT"** por el atraso en el cumplimiento de las obligaciones estipuladas en el presente contrato.

VIGÉSIMA. SANCIONES ADMINISTRATIVAS

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

VIGÉSIMA PRIMERA. SANCIONES APLICABLES Y TERMINACIÓN DE LA RELACIÓN CONTRACTUAL

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

VIGÉSIMA SEGUNDA. RELACIÓN LABORAL

"EL PRESTADOR" reconoce y acepta ser el único patrón del personal que ocupe con motivo de la prestación del servicio objeto de este contrato, así como el responsable de las obligaciones derivadas de las disposiciones legales y demás ordenamientos en materia de trabajo y seguridad social. Asimismo, **"EL PRESTADOR"** conviene en responder de todas las reclamaciones que sus trabajadores presenten en su contra o en contra de **"EL INSTITUTO FONACOT"**, en relación con la prestación del servicio materia de este contrato.

VIGÉSIMA TERCERA. EXCLUSIÓN LABORAL

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

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

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

VIGÉSIMA CUARTA. SUSPENSIÓN DE LA PRESTACIÓN DE LOS SERVICIOS.

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

Cuando la suspensión obedezca a causas imputables a **"EL INSTITUTO FONACOT"**, a solicitud escrita de **"EL PRESTADOR"**, cubrirá los gastos no recuperables, durante el tiempo que dure esta suspensión, para lo cual **"EL PRESTADOR"** deberá presentar dentro de los 30 (treinta) días naturales siguientes de la notificación del término de la suspensión, la factura y documentación de los gastos no recuperables en que haya incurrido, siempre que estos sean razonables, estén debidamente comprobados y se relacionen directamente con el contrato.

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

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

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

VIGÉSIMA QUINTA. RESCISIÓN

"EL INSTITUTO FONACOT" podrá en cualquier momento rescindir administrativamente el presente contrato y hacer efectiva la fianza de cumplimiento, cuando **"EL PRESTADOR"** incurra en incumplimiento de sus obligaciones contractuales, sin necesidad de acudir a los tribunales competentes en la materia, por lo que, de manera enunciativa, más no limitativa, se entenderá por incumplimiento:

a) Si incurre en responsabilidad por errores u omisiones en su actuación;
b) Si incurre en negligencia en la prestación de los servicios objeto del presente contrato, sin justificación para **"EL INSTITUTO FONACOT"**;
c) Si transfiere en todo o en parte las obligaciones que deriven del presente contrato a un tercero ajeno a la relación contractual;
d) Si cede los derechos de cobro derivados del contrato, sin contar con la conformidad previa y por escrito de **"EL INSTITUTO FONACOT"**;
e) Si suspende total o parcialmente y sin causa justificada la prestación de los servicios del presente contrato o no les otorga la debida atención conforme a las instrucciones de **"EL INSTITUTO FONACOT"**;
f) Si no suministra los servicios en tiempo y forma conforme a lo establecido en el presente contrato y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta;
g) Si no proporciona a **"EL INSTITUTO FONACOT"** o a las dependencias que tengan facultades, los datos necesarios para la inspección, vigilancia y supervisión de los servicios del presente contrato;
h) Si cambia de nacionalidad e invoca la protección de su gobierno contra reclamaciones y órdenes de **"EL INSTITUTO FONACOT"**;
i) Si es declarado en concurso mercantil por autoridad competente o por cualquier otra causa distinta o análoga que afecte su patrimonio;

j) Si no acepta pagar penalizaciones o no repara los daños o pérdidas, por argumentar que no le son directamente imputables, sino a uno de sus asociados o filiales o a cualquier otra causa que no sea de fuerza mayor o caso fortuito;
k) Si no entrega dentro de los 10 (diez) días naturales siguientes a la fecha de firma del presente contrato, la garantía de cumplimiento del mismo;
l) Si la suma de las penas convencionales excede el monto total de la garantía de cumplimiento del contrato y/o de las deducciones alcanzan el 20% (veinte por ciento) del monto total de este instrumento jurídico;
m) Si **"EL PRESTADOR"** no presta los servicios objeto de este contrato de acuerdo con las normas, la calidad, eficiencia y especificaciones requeridas por **"EL INSTITUTO FONACOT"** conforme a las cláusulas del presente contrato y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta;
n) Si divulga, transfiere o utiliza 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 DÉCIMA NOVENA del presente instrumento jurídico;
o) Si se comprueba la falsedad de alguna manifestación contenida en el apartado de sus declaraciones del presente contrato;
p) Cuando **"EL PRESTADOR"** y/o su personal, impidan el desempeño normal de labores de **"EL INSTITUTO FONACOT"**, durante la prestación del servicio, por causas distintas a la naturaleza del objeto del mismo;
q) Cuando exista conocimiento y se corrobore mediante resolución definitiva de autoridad competente que **"EL PRESTADOR"** incurrió en violaciones en materia penal, civil, fiscal, mercantil o administrativa que redunde en perjuicio de los intereses de **"EL INSTITUTO FONACOT"** en cuanto al cumplimiento oportuno y eficaz en la entrega de los servicios del presente contrato; y
r) En general, incurra en incumplimiento total o parcial de las obligaciones que se estipulen en el presente contrato o de las disposiciones de la **"LAASSP"** y su Reglamento.

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

Transcurrido dicho término **"EL INSTITUTO FONACOT"**, en un plazo de 15 (quince) días hábiles siguientes, tomando en consideración los argumentos y pruebas que hubiere hecho **"EL PRESTADOR"**, determinará de manera fundada y motivada dar o no por rescindido el contrato, y comunicará a **"EL PRESTADOR"** 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 **"EL INSTITUTO FONACOT"** por concepto del contrato hasta el momento de rescisión.

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 entregaran 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, **"EL 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.

Al no dar por rescindido el contrato, **"EL INSTITUTO FONACOT"** establecerá con **"EL PRESTADOR"** otro plazo, que le permita subsanar el incumplimiento que hubiere motivado el inicio del procedimiento. El convenio modificatorio que al efecto se celebre deberá atender a las condiciones previstas por los dos últimos párrafos del artículo 52 de la **"LAASSP"**.

Cuando se presente cualquiera de los casos mencionados, **"EL INSTITUTO FONACOT"** quedará expresamente facultada para optar por exigir el cumplimiento del contrato, aplicando las penas convencionales y/o rescindirlo, siendo esta situación una facultad potestativa.

Si se llevara a cabo la rescisión del contrato, y en el caso de que a **"EL PRESTADOR"** se le hubieran entregado pagos progresivos, éste deberá de reintegrarlos más los intereses correspondientes, conforme a lo indicado en el artículo 51 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"**.

"EL PRESTADOR" será responsable por los daños y perjuicios que le cause a **"EL INSTITUTO FONACOT"**.

VIGÉSIMA SEXTA. TERMINACIÓN ANTICIPADA

"EL INSTITUTO FONACOT" podrá dar por terminado anticipadamente el presente contrato, 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 contrato con motivo de una resolución de una inconformidad o intervención de oficio emitida por la Secretaría de la Función Pública, lo que bastará sea comunicado a **"EL PRESTADOR"** con 30 (treinta) días naturales anteriores al hecho. En este caso, **"EL INSTITUTO FONACOT"** a solicitud escrita de **"EL PRESTADOR"** cubrirá los gastos no recuperables, siempre que estos sean razonables estén debidamente comprobados y relacionados directamente con el contrato.

VIGÉSIMA SÉPTIMA. DISCREPANCIAS

"LAS PARTES" convienen que, en caso de discrepancia entre la solicitud de cotización, la propuesta económica de **"EL PRESTADOR"** y el presente contrato, prevalecerá lo establecido en la solicitud de cotización respectiva, de conformidad con lo dispuesto por el artículo 81 fracción IV, del Reglamento de la **"LAASSP"**.

VIGÉSIMA OCTAVA. CONCILIACIÓN.

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

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

VIGÉSIMA NOVENA. DOMICILIOS

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

TRIGÉSIMA. LEGISLACIÓN APLICABLE

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

TRIGÉSIMA PRIMERA. DE LA INSPECCIÓN Y VERIFICACIÓN.

"El PRESTADOR" *se obliga a entregar la información o documentación relacionada con el presente contrato, cuando así lo solicite el Órgano Interno de Control en el INSTITUTO FONACOT o demás órganos fiscalizadores o autoridades que ejercen facultades de supervisión al INSTITUTO FONACOT, con motivo de las auditorías, visitas o inspecciones practicadas, de conformidad con lo establecido en los artículos 57 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"*

TRIGÉSIMA SEGUNDA. JURISDICCIÓN

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

Por lo anteriormente expuesto, tanto **"EL INSTITUTO FONACOT"** como **"EL PRESTADOR"**, declaran estar conformes y bien 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 por triplicado en la Ciudad de México, el día 22 de agosto de 2022.

POR "EL INSTITUTO FONACOT"

C. ERIKA HELENA PSIHAS VALDÉS
APODERADA LEGAL Y ÁREA CONTRATANTE

POR "EL PRESTADOR"

C. ALLAN MORGAN VELASCO
APODERADO LEGAL

ADMINISTRADOR DEL CONTRATO

C, HORACIO SÁNCHEZ TINOCO
SUBDIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

ANEXO I
ANEXO TÉCNICO

ANEXO TÉCNICO

"Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones"

TABLA DE CONTENIDO

1. DESCRIPCIÓN DEL SERVICIO

1.1 ANTECEDENTES.

El Instituto FONACOT, es una organización que fomenta el desarrollo integral de los trabajadores y el crecimiento de su patrimonio familiar, promoviendo el acceso al otorgamiento de créditos a los trabajadores formales, para la obtención de bienes y servicios a precios competitivos.

Asimismo, derivado de los servicios proporcionados en años anteriores, al área de la Subdirección General de Tecnologías de la Información y Comunicación (SGTIC) con respecto al "**Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones**" que le ha permitido al Instituto la correcta remediación, control y mitigación de riesgos, y amenazas así como el establecimiento de herramientas, metodologías y personal de seguridad de la información para atender, solucionar, remediar, mitigar los posibles eventos que pudiesen presentarse durante la vigencia del servicio integral.

2. JUSTIFICACIÓN.

El Instituto FONACOT requiere mantener la Operación del **"Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones"**, para dar continuidad a sus procesos y procedimientos conforme a las normas, regulaciones y las mejores prácticas de seguridad de la información.

Para asegurar la adecuada administración, control y mitigación de los hallazgos, el LICITANTE deberá mantener la operación en el Instituto FONACOT, de los servicios enunciados en el **Numeral 5. Descripción General del Servicio**.

3. ALCANCE DEL SERVICIO

3.1 Continuidad Operativa

El Instituto FONACOT requiere continuar con las operaciones en el rubro de la seguridad de la información inmerso en todos los elementos de las Tecnologías de la Información y Comunicaciones que brindan apoyo a los servicios que se les proporciona a los trabajadores formales en el proceso de otorgamiento de créditos, procesos adyacentes a este y dar cumplimiento a las normas, regulaciones y estándares que permitieron la correcta y segura operación del Instituto

A fin de establecer las mejores condiciones para la prestación de los Servicios de Seguridad de la Información, el licitante, deberá de verificar y mantener los servicios para la correcta operación del Instituto.

El horario de operaciones en las localidades de Oficinas Centrales y Plaza de la Republica del Instituto FONACOT es de 8:00 a 21:00 horas de lunes a viernes y de 8:00 a 17:00 horas sábados.

El resto de las localidades operan en un horario de 8:00 a 20:00 horas de lunes a viernes y de 8:00 a 17:00 horas los sábados hora local.

4. SERVICIOS BAJO DEMANDA

El Instituto FONACOT de conformidad con las necesidades de operación, podrá requerir al LICITANTE ganador, servicios bajo demanda, a través de una solicitud expresa del Administrador del Contrato.

Los servicios que suministre el LICITANTE ganador bajo este concepto deberán cumplir con las características técnicas que se describen en este anexo técnico y estas se deberán tomar como referencia para el suministro de equipos y soluciones, considerando que en función al constante desarrollo tecnológico, los activos a entregar durante el periodo que abarca el servicio deberán ser provistos con características iguales o superiores, y que en ninguno de los casos deberán ser por debajo de las características técnicas establecidas en este anexo técnico, debiéndose proveer todas licencias, interfaces, cables de corriente, componentes, dispositivos, software operativo del hardware, drivers, etc., que permitan su adecuada operación.

Para los servicios bajo demanda, se tomarán como referencia los costos unitarios presentados en la propuesta económica del LICITANTE ganador, independientemente de la fecha en que se solicite el servicio. El Instituto notificará al LICITANTE al menos diez días antes de la baja de cualquiera de los servicios descritos en este Anexo Técnico.

Para los servicios bajo demanda, el LICITANTE, deberá considerar lo referente a instalación, puesta a punto, administración, soporte técnico, mantenimiento preventivo, garantías, licenciamiento, accesorios y cualquier otro elemento que sea necesario para el otorgamiento de los servicios.

Los servicios descritos en el numeral **5. Descripción General del Servicio**, presente Anexo, estarán considerados en un esquema bajo demanda:

1 Servicio de Gestión, Seguimiento y Control de Incidentes.
2 Servicio de Validación de Identidad.
3 Servicio de Detección e Investigación de Vulnerabilidades y Pruebas de Penetración.
4 Servicio de Control y Gestión de usuarios.
5 Servicio de Protección de bases de datos.
6 Servicio de Administración del MGSI.

5. DESCRIPCIÓN GENERAL DEL SERVICIO.

El **"Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones"**, para el Instituto FONACOT, integra una serie de servicios que deberán llevarse a cabo para minimizar el impacto de cualquier evento o incidente de seguridad de la información que llegara a suscitarse en la infraestructura tecnológica del Instituto, afectando las propiedades de disponibilidad, integridad y confidencialidad de los activos de información institucionales.

El **"Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones"**, está integrado por los siguientes servicios:

1 Servicio de Gestión, Seguimiento y Control de Incidentes.
2 Servicio de Validación de Identidad.
3 Servicio de Detección e Investigación de Vulnerabilidades y Pruebas de Penetración.
4 Servicio de Control y Gestión de usuarios.
5 Servicio de Protección de bases de datos.
6 Servicio de Administración del MGSI.

El LICITANTE deberá contar con los recursos necesarios para llevar a cabo el **"Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones"**, a través de personal especializado y certificado conforme a los perfiles descritos en este Anexo Técnico.

6. SERVICIO DE GESTIÓN, SEGUIMIENTO Y CONTROL DE INCIDENTES.

6.1 Descripción del Servicio

El Instituto FONACOT requiere de un servicio de gestión, seguimiento y control de incidentes para los servicios inherentes a los términos de seguridad.

El LICITANTE deberá proporcionar el equipamiento y su respectivo mantenimiento preventivo y correctivo de la infraestructura asegurando la correcta ejecución del servicio con los siguientes perfiles: un CyberSecurity leader y un Specialist incident handler.

EL LICITANTE deberá llevar a cabo la recolección y correlación de eventos de los servicios inherentes a los términos de seguridad y otras fuentes de información para la detección de ataques en tiempo real y el Especialista en gestión de servicios y seguridad de la información será el responsable de realizar la configuración de parámetros, reglas y políticas que permitan detectar actividad maliciosa dentro de la red e infraestructura del Instituto FONACOT.

EL LICITANTE, deberá integrar un análisis de comportamiento de usuario, que permita ayudar a detectar y responder a las amenazas de usuarios internos, reducir falsos positivos y priorizar las amenazas con mayor nivel de riesgo.

EL LICITANTE deberá implementar las soluciones respectivas en el Centro de Datos del Instituto para estar en condiciones de realizar la gestión, seguimiento y control de incidentes para los servicios inherentes a los términos de seguridad.

6.2 Características del Servicio

5.2.1 El LICITANTE deberá contar con un centro de datos y área de operación dentro de sus instalaciones para asegurar la operación de los servicios ofertados con la finalidad de garantizar los niveles de servicio requeridos por el Instituto. Lo referido con antelación deberá disponer de las siguientes características:

- Centro de datos:
  - Sistema de video vigilancia.
  - Sistema de control de acceso físico deberá ser a través de controles biométricos o automatizados.
  - Sistema de energía ininterrumpida (UPS) y al menos planta de emergencia.
  - Cableado estructurado nivel 6 o superior.
  - Sistema de aire acondicionado de alta precisión.
  - Sistema de detección y supresión de fuego.
  - Sistema de monitoreo ambiental. (humedad, condiciones anómalas de accesos y electricidad, temperatura).

- Área de operación:
  - Deberá estar separada de la red del licitante.
  - Deberá ser de acceso exclusivo para el personal que realiza el servicio.
  - Deberá alojar únicamente al personal que realiza el servicio.
  - El control de acceso deberá ser a través de controles biométricos o automatizados.

- Infraestructura del área de operación:
  - Consola de monitoreo para visualizar los eventos o incidentes inherentes a los servicios ofertados.
  - Herramientas de monitoreo en tiempo real de la disponibilidad de los equipos para los servicios inherentes ofertados.
  - Sistema de administración de tickets para la atención de solicitudes.

- Tableros de control con pantallas dedicadas para el monitoreo de los servicios inherentes ofertados.

5.2.2 Los servicios de gestión, seguimiento y control de incidentes se realizarán de manera remota y deberán efectuar al menos las siguientes actividades:

- Detectar, analizar y escalar eventos e incidentes de seguridad para los servicios inherentes, con una cobertura en formato de 24x7x365.
- Realizar la identificación y caza de amenazas reportadas en la infraestructura de los servicios inherentes de seguridad, permitiendo dar respuestas a preguntas como: ¿Cómo empezó el problema?, ¿Qué actividades realizó la amenaza?, ¿Existen dispositivos infectados?, ¿Cómo se puede resolver la amenaza? Integrando información que se obtenga del Servicio de aseguramiento de identidad Institucional.
- Atender requerimientos relacionados con los servicios inherentes de seguridad.
- Realizar respuesta a incidentes de seguridad, con los perfiles del personal especializado.
- Detectar y detener ataques de seguridad conforme al alcance de los servicios inherentes de seguridad.
- Seguimiento y control del rendimiento de los componentes de seguridad del servicio, asegurándose que operen bajo condiciones normales (CPU, memoria, disco duro, los cuales se mencionan de manera enunciativa más no limitativa).

5.2.3 El LICITANTE deberá considerar los ingenieros de fortalecimiento de TI necesarios en las instalaciones del Instituto FONACOT para asegurar la correcta operación, gestión, seguimiento y control de los servicios inherentes a los servicios de seguridad del instituto en un horario que se acordará entre el licitante ganador y el LICITANTE Instituto FONACOT:

- Un primer nivel para las operaciones diarias y configuraciones comunes, atención de requerimientos y ajustes requeridos a las distintas soluciones tecnológicas del instituto, detección de eventos y análisis, tareas de tipo administrativas, escalamiento de eventos relevantes, atención de tickets y llamadas telefónicas del instituto.
- Un segundo nivel para las operaciones enfocadas en la investigación sobre datos con base en reportes de inteligencia, así como para el análisis detallado de los eventos relevantes reportados por el grupo de primer nivel y la atención de respuesta a incidentes.
- El personal deberá ser capaz de recibir y analizar reportes de amenazas, incidentes y alertas de vulnerabilidades. El análisis deberá incluir acciones específicas para aplicarse en el entorno de TI.
- El personal deberá analizar e identificar eventos anómalos que son detectados por las soluciones administradas, integrar resultados, datos e información proporcionada por el instituto proveniente de otras soluciones tecnológicas, con el fin de complementar y ampliar los resultados del análisis.
- El personal deberá recibir y analizar noticias relacionadas con la seguridad de la información. Así mismo, deberá contar con diversas fuentes de inteligencia de amenazas (Threat Intelligence Feeds) propias y/o de fabricantes y fuentes abiertas para generar:
  - Alertas de vulnerabilidad.
  - Indicadores sobre la actividad de amenaza cibernéticas y mitigaciones recomendadas.
- El personal de seguridad de la información deberá utilizar los mecanismos para la atención y administración del grupo resolutor, sobre la cual se haga el registro y seguimiento de requerimientos, incidentes, y tareas que deberá atender a través de llamadas telefónicas y correos electrónicos de la Mesa de Servicios institucional que cuenta el Instituto FONACOT.
- El personal de seguridad de la información deberá entregar durante los primeros 6 días hábiles de cada mes, los reportes asociados a la administración y control de los incidentes y solicitudes que le fueron asignados de la Mesa de Servicios del Instituto FONACOT.

- El personal deberá realizar la actualización y el respaldo periódico de las configuraciones de los componentes que integran la solución del servicio propuesta.
- El personal deberá tener conocimiento en la administración y operación de cada una de las soluciones tecnológicas de la institución, a fin de llevar a cabo una correcta operación y gestión diaria de las mismas.
- El personal deberá cumplir con experiencia, competencias, habilidades, cursos y/o certificaciones, los cuales deberán incluirse en la propuesta técnica y estar vigentes.

5.2.4 El servicio deberá considerar la actualización periódica de la totalidad de los componentes de seguridad administrados, y realizar la migración a nuevas versiones de software. En caso de presentarse alguna falla o inestabilidad en los equipos, se deberá reparar o sustituir el componente dañado. El LICITANTE, será responsable de remplazar el hardware y software por fallas, ineficiencia, obsolescencia y/o crecimiento de las soluciones.

5.2.5 El servicio del LICITANTE deberá contemplar un grupo resolutor, el cual recibirá los requerimientos técnicos, incidentes operativos o de seguridad del instituto para cada incidente o requerimiento particular, dicho grupo resolutor deberá estar disponible en un formato de 7 días por 24 horas los 365 días del año.

5.2.6 El LICITANTE deberá priorizar la atención de solicitudes e incidentes en base a los siguientes niveles:

- Nivel Alto.
  - Representan problemas que impidan la continuidad de la operación.
  - Ejemplos: dispositivo no funciona, el dispositivo genera una falla en la operación de la red.
- Nivel Medio.
  - Representan problemas de funcionalidad o eventos que causen una interrupción parcial.
  - Ejemplos: El funcionamiento de la plataforma se encuentra degradada o con errores de ejecución en algunos módulos.
- Nivel Bajo.
  - Representan problemas menores que no interrumpan la operación y que causan una afectación mínima.
  - Ejemplos: El dispositivo tiene un problema menor que no afecta a la operación fundamental del mismo y/o se encuentra alertado.

Nivel	Recepción de la solicitud	Tiempo estimado de recuperación del servicio
Alto	20 minutos	6 horas
Medio	1 hora	24 horas
Bajo	2 horas	48 horas

5.2.7 El servicio deberá considerar las siguientes actividades:

- Integrar fuentes para análisis de eventos.
- Identificar, analizar y correlacionar eventos.
- Definir reglas políticas y umbrales.
- Revisar fuentes de inteligencia para identificar riesgos.
- Definir y desarrollar acciones de mitigación.

5.2.8 El servicio deberá incluir un procedimiento de atención de solicitudes (altas, bajas y cambios), alineado al estándar internacional ISO/IEC 27001, el cual se deberá acreditar mediante la presentación del certificado vigente y a nombre del licitante.

6.3 Descripción de Componentes

6.3.1 El servicio de gestión, seguimiento y control de incidentes deberá brindar el servicio de correlación de eventos y análisis de comportamiento que pueda soportar la cantidad de 5000 mensajes por segundo y considerar la capacidad de almacenamiento de hasta 3 meses en línea para la consulta de información. Adicionalmente, se deberá considerar el almacenamiento fuera de línea de toda la información colectada durante la vigencia del contrato.
6.3.2 La solución deberá permitir la expansión de memoria hasta 128GB.
6.3.3 La solución deberá contener al menos 10 TB de almacenamiento interno.
6.3.4 La solución deberá permitir compresión 20:01.
6.3.5 La solución deberá contener 12 / 24 CPU´s físicos o virtuales.
6.3.6 La solución deberá soportar AC Broadcom 5720 QP (4 x 1Gb) (Ethernet).
6.3.7 La solución deberá soportar al menos 25,000 MPS de capacidad máxima de archivos (Max Archiving Rates).
6.3.8 La solución deberá incluir componentes adicionales para aumentar la tolerancia a errores, la capacidad y el rendimiento.
6.3.9 La solución deberá contar con equipos redundantes y en una configuración de Cluster en alta disponibilidad con conexiones de Fibra (1GB,10GB,40GB) y de cobre de 1GB, para mantener una operación a prueba de paros y a prueba de fallas.
6.3.10 La solución deberá contar por cada unidad con fuentes de poder redundantes internas y alimentadas ya sea con 120 ó 240 VAC. Además, de ser reemplazables en caliente sin pérdida de servicio.
6.3.11 La solución deberá contar por cada unidad con ventiladores para flujo de aire.
6.3.12 La solución deberá tener al menos 16 puertos de Fibra Giga Ethernet para el uso de herramientas.
6.3.13 La solución deberá contar por unidad el poder de instalarse en racks, y si lo requiriere contar con charolas para su correcta instalación.
6.3.14 La solución deberá contar con la capacidad de recibir módulos con puertos ópticos de fibra (1,10 y 40) de tecnología GE.
6.3.15 La solución deberá contar con un puerto de consola y al menos un puerto 10/100/1000BaseTX para administración.
6.3.16 La solución deberá contar con un GUI (interface de usuario) grafica e intuitiva de fácil operación y configuración.
6.3.17 Los equipos propuestos en la solución deberán disponer de recursos de procesamiento y memoria independiente para la gestión.
6.3.18 Los equipos propuestos en la solución deberán contar con la certificación FIPS 140-2.
6.3.19 Los equipos propuestos en la solución deberán contar con la certificación Common Criteria.
6.3.20 La solución deberá incluir todas las licencias requeridas para el completo y correcto funcionamiento de toda la solución en general por tres años.
6.3.21 Los equipos propuestos de la solución deberán contar con el mismo Sistema Operativo.
6.3.22 La solución propuesta deberá incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de cortado de tráfico.
6.3.23 La solución propuesta deberá incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de visibilidad de sesiones cifradas.
6.3.24 La solución propuesta deberá incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de enmascaramiento de tráfico.
6.3.25 La solución propuesta deberá incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de identificación de puerto de origen.
6.3.26 La solución propuesta deberá incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de creación de túneles seguros.
6.3.27 La solución propuesta deberá incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de supresión de encapsulados.
6.3.28 La solución propuesta deberá incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de duplicación de paquetes.

6.3.29 La solución propuesta deberá incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de generación 1:1 de paquetes tipo FLOW.

6.3.30 La solución propuesta deberá incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de agregación de etiquetas a los paquetes con el fin de medir el tiempo de respuesta.

6.3.31 Los artefactos contemplados en este esquema de solución deberán contener las características y especificaciones del soporte y pólizas de mantenimiento de los mismos.

6.4 Descripción de Funcionalidades

6.4.1 La solución deberá considerar un dispositivo de administración de información y eventos de seguridad en las instalaciones del Instituto FONACOT, mismo que debe estar considerado dentro del "cuadrante mágico de Gartner" para el año 2017 y categorizado como "Leader".

6.4.2 La solución deberá proveer en términos generales las siguientes capacidades integradas en una misma interface de administración personalizable y basada en web:

- Monitoreo de Seguridad.
- Investigación basada en metadatos de eventos de seguridad y captura de tráfico.
- Reconstrucción de sesiones en el caso de que se requiera un análisis en profundidad forense.
- Reportes para Cumplimiento normativo.

6.4.3 La solución de Inteligencia de Seguridad (Security Intelligence) con la que se aprovisione la solución deberá contar con las siguientes capas en cuestión de arquitectura y diseño:

- Colección
- Administración de Logs (Log Management)
- Administración de Eventos (Event Management)
- Correlación de eventos
- Alarmas
- Manejo de Incidentes y casos
- Manejo de flujos de trabajo con posibilidad de automatización
- Reporteo
- Análisis forense de la red (Network Forensics)

6.4.4 La solución no deberá en ningún momento acceder a soluciones externas para brindar las funcionalidades aquí expresadas.

6.4.5 La solución deberá permitir acceder a los logs originales (raw log data), siempre que así se desee, además de contar con la información previamente interpretada por la solución de Inteligencia de Seguridad / Security Intelligence (Eventos, Alarmas e Incidentes).

6.4.6 La solución deberá contar con la posibilidad de que la consola administrativa sea accesible por Internet Explorer/Chrome/Firefox/Safari vía web (HTTPS).

6.4.7 La solución deberá contar con la posibilidad de distribuirse geográficamente en distintas locaciones conteniendo integridad en la información que está siendo analizada. La solución deberá mantener cifrado en los componentes de autenticación y en las capas de transporte de datos, este cifrado podrá ser desactivado en algunos componentes para proveer funcionalidades de agilización de transferencias de datos.

6.4.8 La solución deberá permitir un modelo de (delivery) entrega basado en: Appliance.

6.4.9 La solución deberá estar basada en una plataforma endurecida (Hardened) de sistema operativo (preferiblemente Windows), dicho sistema operativo debe estar en cumplimiento con Common Criteria EAL2 (Methodically designed, tested and checked), en caso de tratarse de soluciones basadas en Linux, deberá validarse el cumplimiento y soporte de los mismos.

6.4.10 La solución deberá poder aplicar parches al sistema operativo de manera discrecional conforme recomendaciones del fabricante del sistema operativo, sin impactar el rendimiento y presentación de la aplicación, el fabricante de la solución de Inteligencia de Seguridad / Security Intelligence, no deberá de ninguna manera regular el acceso a los parches de sistema operativo y componentes específicos alternos a la solución ofertada.

6.4.11 La solución deberá coleccionar logs de las plataformas además de poderlo realizar de forma "agentless" sin agentes, o de manera hibrida en un deployment específico.

6.4.12 Los componentes de las soluciones propuestas deberán estar certificados por el fabricante, además de disponibles para plataformas:

- Windows Server 2003 (32 Y 64 Bits)
- Windows Server 2008 (32 Y 64 Bits)
- Windows Server 2008 R2 (64 Bits)
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Vista (32 y 64 Bits)
- Windows XP (32 Bits)
- Windows 7 (64 Bits)
- Windows 8
- Windows 10
- Linux RedHat Enterprise
- Solaris
- HP-UX
- AIX

6.4.13 La solución deberá soportar colección de plataformas ampliamente utilizadas de manera nativa como son:

- Windows Events Remote Collection
- Netflow v1,v5,v9, IPFIX
- Cisco IDS (vía SDEE)
- Checkpoint LEA
- Fortinet
- Sourcefire eStreamer
- Nessus API
- Nexpose API
- AS400 (iSeries), z/OS (zSeries), GuardianOS (Tandem), etc.

6.4.14 La solución de Inteligencia de Seguridad (Security Intelligence), deberá contar con la posibilidad de poder manejar una capa de información viva (live data) para búsquedas avanzadas y detalladas y una capa de información en reposo (cold data) siempre permitiendo utilizar datos viejos archivados fuera de la infraestructura en reportes e investigaciones forenses inclusive hasta 10 años.

6.4.15 La solución de Inteligencia de Seguridad (Security Intelligence), deberá acoplarse a utilizar las soluciones de STORAGE NAS/SAN del Instituto FONACOT, sin necesidad de sustituirlas por las soluciones propietarias.

6.4.16 La solución no deberá presentar ningún tipo de costo extra a la adquisición de STORAGE ni mucho menos representar este costo en la propuesta económica para la utilización del STORAGE ya adquirido o en el esquema que este contemplado por el Instituto FONACOT.

6.4.17 Los logs archivados de la solución deberán tener la funcionalidad de almacenarse y deberán tener la tipificación básica de evidencia legal bajo el concepto (digital chain of custody) todo ello por medio de la no alteración y la custodia de los logs originales.

6.4.18 La solución deberá realizar funciones normalización y mediación en su capa de administración de logs (log management) no en su capa de colección para aminorar el impacto a los equipos que realizan las funciones de colección.

6.4.19 La solución deberá poder separar lo archivado por entidad e infraestructura con fines de poder gestionar backups de esos archivos de manera separada sin impactar los backups generales de la plataforma, lo anterior tiene el fin de que la solución muestre un arreglo de multi tenencia (Multi-Tenant) donde las bitácoras archivadas se puedan separar de manera general por cliente, edificio o grupo, dependiendo la configuración que se plantee, sin tener que trabajar con la plataforma completa.

6.4.20 Cuando en la solución la cantidad de logs recibida sobrepase la capacidad licenciada de logs la solución NO deberá "tirar/borrar" los logs sino meterlos en un proceso de espera para su procesamiento futuro cuando su carga baje.

6.4.21 La solución deberá contar con un framework o método sencillo para poder integrar nuevos dispositivos no detectados conforme necesidades futuras de la institución en cuestión de normalización de bitácoras.

6.4.22 El sistema de administración de logs de la solución deberá contar con la posibilidad de configurar que es un evento y que no, de todos los logs que se reciben, con fines de maximizar las capacidades de análisis de información importante e información intrascendente.

6.4.23 El sistema de administración de logs de la solución deberá proporcionar la posibilidad de rotar con funcionalidades de alta disponibilidad y saturación a los agentes entre el pool de manejadores de logs de manera automatizada para que, si los agentes pierden conectividad con el manejador de logs A, el manejador de logs B los reciba sin problema alguno y más tarde sincronicen sus colecciones, cuando el manejador de logs A regrese.

6.4.24 El sistema de administración de logs de la solución deberá contar con la posibilidad de traducir de manera automatizada y en tiempo real PAISES, ESTADOS y CIUDADES en vez de mostrar solo direcciones IP para los eventos que sean reenviados al sistema de administración de eventos.

6.4.25 El producto de Inteligencia de Seguridad (Security Intelligence) de la solución deberá poder brindar auto-clasificación de los datos capturados en modo estructurado con fines de brindar funcionalidades de búsquedas estructuradas (structured search), pero también brindar funcionalidades de búsqueda no estructurada, esto quiere decir que el sistema de inteligencia podrá ser consultado en función de estructuras específicas de datos conocidas pero también deberá permitir consultar datos sin conocer su estructura (unstructured search), lo anterior deberá estar presente en un producto único sin necesidad de duplicar la información.

6.4.26 La solución deberá detectar y neutralizar amenazas conocidas y desconocidas basadas en el usuario. Esto es, de manera enunciativa más no limitativa, exponer las amenazas internas, cuentas comprometidas y el uso indebido y abuso de privilegios, todo en tiempo real.

6.4.27 La solución deberá distinguir entre cuentas de usuario legítimas y comprometidas mediante la identificación de actividad anómala.

6.4.28 La solución deberá supervisar e informar automáticamente sobre la creación de cuentas con privilegios y la elevación de permisos.

6.4.29 La solución deberá detectar cuándo un usuario accede indebidamente a datos protegidos.

6.4.30 La solución deberá correlacionar la información de registro con identidades únicas que permitan conocer quién está detrás una acción maliciosa.

6.4.31 La solución deberá tener la capacidad de crear líneas de base que se usen para detectar el comportamiento anómalo a través del aprendizaje automático y técnicas de análisis estadístico.

6.4.32 La solución deberá usar inteligencia artificial y tecnologías de aprendizaje automático que permitan mejorar el tiempo de detección y respuesta a amenazas.

6.4.33 La solución deberá proporcionar administración de casos, investigación de incidentes y generación de reportes exhaustivos.

6.4.34 La solución deberá ser capaz de soportar instancias virtuales independientes (KVM, VMWARE) así como que permitan la integración de plataformas basadas en la nube de tipo openstack y Cisco ACI.

6.4.35 La solución deberá ser capaz de soportar la modificación, manipulación, transformación y transporte de paquetes de las capas 2,3,4 del modelo de referencia OSI.

6.4.36 La solución deberá de ser capaz de crear filtrado de patrones basados en los atributos definidos de usuario (UDA).

6.4.37 La solución deberá contar con integración de BYPASS externo físico y lógico.

6.4.38 La solución deberá contar con la activación de todas las funcionalidades de forma concurrente en todos los puertos y equipos solicitados.

6.4.39 La solución deberá poder realizar modificación, manipulación, transformación y transporte de paquetes de las capas 2, 3, 4 del modelo de referencia OSI.

6.4.40 La solución deberá de ser capaz de crear filtrado de patrones basados en los atributos definidos de usuario (UDA).

6.4.41 La solución deberá poder seleccionar, modificar, manipular, transformar y transportar de tráfico específico a cada una de las herramientas para las capas 2, 3, 4 del modelo de referencia OSI.

6.4.42 La solución deberá permitir la autenticación de los usuarios administradores mediante RADIUS, TACACS, LDAP y base de datos LOCAL.
6.4.43 La solución deberá mediante el uso de mapas administrados por usuario (RBAC), permitir el aprovechamiento de un mismo puerto para distintos usos.
6.4.44 La solución deberá soportar el manejo de tráfico Multicast a varios puertos permitiendo así el acceso del mismo tráfico a distintas herramientas conectadas.
6.4.45 La solución deberá soportar el estándar IEEE 802.1Q (encapsulado de varias vlans sobre el mismo enlace físico).
6.4.46 5La solución deberá soportar el estándar IEEE 802.3ad (agregación de varios enlaces físicos).
6.4.47 La solución deberá soportar Jumbo Frames (MTU 9000 bytes).
6.4.48 La solución deberá soportar IPv6 e IPv4.
6.4.49 La solución deberá proteger el tráfico (Inline) de todas las herramientas (Firewalls, IPS, antimalware, SSL encryption) conectadas en los puertos de los equipos propuestos.
6.4.50 La solución deberá soportar la relación inline de muchos a muchos.
6.4.51 La solución deberá soportar la capacidad de creación de CLUSTER con otras plataformas del mismo fabricante y deberán ser administrados por la misma consola.
6.4.52 La solución deberá soportar al menos los siguientes tipos de conectores: SFP, SFP+, QSFP+, QSFP28 incluyendo los siguientes tipos de cables: SR, LR, ER, BIDI.
6.4.53 La solución deberá soportar la capacidad NON BLOCKING en los STACKS con otras soluciones similares del mismo fabricante.
6.4.54 La solución deberá soportar la capacidad NON BLOCKING en el BACKPLANE de la plataforma ofertada.
6.4.55 La solución deberá contar con módulos intercambiables en caliente (HOTSWAP).
6.4.56 La solución deberá poder clasificar el tráfico en tiempo real identificando geolocalización y tipo de equipo.
6.4.57 La solución deberá tener balanceo de cargas para tráfico en línea y tráfico en paralelo.
6.4.58 La solución deberá poder terminar túneles de GRE para una comunicación alterna y así soportar una alta disponibilidad de las interconexiones de red.
6.4.59 El licitante deberá entregar de manera mensual un reporte de inteligencia con los siguientes rubros:

- Introducción
- Alcance
- Descripción
- Tendencias de ataques
- Detalle Servicio Sitio 1
- Detalle Servicio Sitio 2
- Detalle Servicio Sitio 3
- Detalle Servicio Sitio 4
- Perfil de los ataques
- Incidentes Relevantes
- Acciones de respuesta
- Perfil de los atacantes
- Recomendaciones Generales
- ANEXOS
- GLOSARIO

7. SERVICIO DE VALIDACIÓN DE IDENTIDAD.

7.1 Descripción del Servicio

El **"Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones"**, deberá permitir al Instituto FONACOT realizar validación de identidad de los **beneficiarios** que tramiten un crédito y de esta manera reducir los tiempos y los riesgos financieros derivados de la ejecución de las transacciones

electrónicas, tales como los fraudes por robo de identidad. El servicio deberá permitir al Instituto FONACOT estar en condiciones de cumplir con las regulaciones y normas mexicanas aplicables.

7.2 Características del Servicio

7.2.1 Derivado de la sensibilidad de los trámites de crédito que realiza El Instituto FONACOT, el servicio de validación de identidad propuesto por el LICITANTE deberá estar soportado por un producto de fabricante que cuente con base instalada y no se aceptará que sea desarrollo de software a la medida.

7.2.2 El servicio de validación de identidad deberá poder integrarse con los dispositivos biométricos y estaciones de trabajo con los que ya cuenta la plataforma tecnológica del Instituto FONACOT, para el uso desde las sucursales y las diferentes caravanas.

7.2.3 El servicio de validación de identidad deberá ser supervisado por el especialista en validación de identidad y contemplará el análisis para el desarrollo de casos de uso y su incorporación con los dispositivos biométricos y los sistemas del Instituto FONACOT.

7.2.4 En el momento que El Instituto FONACOT requiera el servicio de validación de identidad, la solución propuesta por el Licitante, deberá cumplir con las bases y mecanismos técnicos necesarios establecidos por el Instituto Nacional Electoral (INE), que permita la verificación de los datos contenidos en la credencial para votar y de las minucias de las huellas digitales de los ciudadanos registrados en el Padrón Electoral.

7.2.5 En el momento que El Instituto FONACOT efectúe el acuerdo para realizar validación de identidad contra el Padrón Electoral del INE, facilitará al LICITANTE las características del hardware de seguridad que integrará con el INE y la solución de validación de identidad deberá contar con la capacidad de integración con las mismas. Esta infraestructura será proporcionada por El Instituto FONACOT (firewalls, enlaces, servidores, dispositivos de validación de identidad móviles y equipos biométricos).

7.2.6 El servicio de validación de identidad deberá autenticar, cifrar, y firmar electrónicamente las peticiones de consulta de los puntos de verificación y validación hacia el (INE).

7.2.7 El servicio deberá realizar funciones de auditoría para validar la integridad de la información ante una posible controversia derivado de las peticiones de consulta.

7.2.8 El servicio deberá mantener y ofrecer el monitoreo de las transacciones a lo largo de todo el proceso de consulta.

7.2.9 El servicio deberá cumplir con la emisión de sellos de tiempo conforme al estándar RFC 3161 para cada solicitud de consulta generada.

7.2.10 El servicio deberá realizar la validación de documentos oficiales como comprobantes de domicilio, recibos de nómina, y estados de cuenta a través de archivos XML.

7.2.11 La solución propuesta deberá tener la capacidad de personalizar las interfaces web de acuerdo con la imagen institucional del Instituto FONACOT.

7.2.12 El servicio deberá tener la capacidad de realizar validaciones con entidades de verificación de información, como: RENAPO, SAT e INE principalmente.

7.2.13 El servicio deberá tener la capacidad de brindar una identidad digital a personas y equipos a través de certificados digitales X.509. y deberá estar en condiciones de resguardar las llaves correspondientes en módulos de seguridad en hardware (HSMs).

7.2.14 El servicio deberá tener la capacidad de otorgar visibilidad sobre el estado de dispositivos de seguridad en hardware (HSMs). Así mismo, deberá ofrecer un esquema de monitoreo en intervalos de tiempo de al menos un minuto.

7.2.15 El servicio deberá tener la capacidad de generar las alertas correspondientes a dicho monitoreo de acuerdo con los parámetros de criticidad definidos por El Instituto FONACOT.

7.2.16 El servicio deberá permitir la implementación de dominios de trabajo para segmentar y delimitar el acceso de los componentes del servicio.

7.2.17 El servicio deberá tener la capacidad de integrarse con dispositivos que realicen la validación física de credenciales para votar y pasaportes.

7.2.18 La solución de validación de identidad del LICITANTE deberá cumplir con los siguientes estándares:

- Llaves públicas y privadas RSA a 1024/2048/4096 bits.

- Certificados digitales X509 v3.
- Estándares de criptografía PKCS#1, PKCS#7, CAdES, SAdES y PAdES.
- Algoritmos de digestión MD5, SHA-I, SHA-256.
- Protocolo para consulta de estado de revocación de certificados digitales (OCSP RFC 2560).
- Listas de certificados revocados (CRL — RFC 3280).
- Estampillas de Tiempo (TSP - RFC 3161).
- Integración con dispositivos criptográficos de seguridad HSM a través del estándar PKCS#11.

7.3 Descripción de Componentes

7.3.1 La solución deberá cumplir con los estándares de seguridad UL, CE, FCC, C-TICK, Canadá ICES, RoHS2 y WEEE.
7.3.2 La solución deberá soportar API´s PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG.
7.3.3 La solución deberá soportar algoritmos criptográficos asimétricos RSA, Diffie-Hellman, ECMQV, DSA, KCDSA, ECDSA, ECDH.
7.3.4 La solución deberá soportar algoritmos criptográficos simétricos AES, AES-GCM, ARIA, Camellia, CAST, RIPEMD160 HMAC, SEED, Triple DES.
7.3.5 La solución deberá contar con los cumplimientos de seguridad FIPS 140-2 Level 2 and Level 3, USGv6 accreditation.
7.3.6 La solución deberá soportar los sistemas operativos:

- Microsoft Windows 7 x64, 10 x64
- Windows Server 2008 R2 x64, 2012 R2 x64, 2016 x64
- 2016 Nano x64¡
- Red Hat Enterprise Linux Server 6 x64, x86 and Server 7 x64
- SUSE Enterprise Linux 11 x64, 12 x64
- Linux AS/ES 5 x64 (libc6.5)
- Oracle Solaris 11 SPARC 64
- Oracle x86 running Solaris 11 x64 IBM AIX 7.1 (POWER6, POWER8)
- HP-UX 11i V3 ITANIUM Oracle Enterprise Linux 6.8 and 7.1 Virtual environment support:
  - Microsoft Windows Hyper-V Server 2012 R2,
  - 2016 VMware ESXi 5.5
  - Citrix XenServer 6.5
  - AIX LPARs

7.3.7 La solución deberá soportar alta disponibilidad (HA).
7.3.8 La solución deberá soportar un consumo de energía, up to 2.0A at 110V AC, 60Hz | 1.0A at 220V AC, 50Hz.
7.3.9 La solución deberá soportar altas capacidades de transacción dónde el rendimiento es crítico.
7.3.10 Los artefactos contemplados en este esquema de solución deberán contener las características y especificaciones del soporte y pólizas de mantenimiento de los mismos.

7.4 Descripción de Funcionalidades

7.4.1 La solución deberá realizar funciones tales como cifrado, generación y protección de claves en aplicaciones, incluidas de manera enunciativa mas no limitativa, las autoridades de certificación, la firma de códigos y el software personalizado.
7.4.2 La solución deberá permitir el almacenamiento y procesamiento seguro de llaves y aplicaciones.
7.4.3 La solución deberá poder realizar descarga y aceleración criptográfica.
7.4.4 La solución deberá proporcionar control de accesos multinivel autenticado.
7.4.5 La solución deberá permitir autenticación de cliente utilizando hardware token.
7.4.6 La solución deberá poder realizar copia de seguridad, replicación y recuperación de la llave.

7.4.7 La solución deberá brindar un almacenamiento ilimitado de llaves protegidas.
7.4.8 La solución deberá soportar agrupamiento y balanceo de carga.
7.4.9 La solución deberá poder realizar separación criptográfica lógica de las llaves de la aplicación.
7.4.10 La solución deberá tener la capacidad de realizar autenticación multifactor.

8. SERVICIO DE DETECCIÓN E INVESTIGACIÓN DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN.

8.1 Descripción del Servicio

EL LICITANTE deberá proveer una solución de detección e investigación de vulnerabilidades de la infraestructura y aplicaciones informáticas del Instituto FONACOT, así como verificar que se cumpla con las mejores prácticas de desarrollo seguro de software.

EL LICITANTE deberá Identificar y solucionar problemas de seguridad, vulnerabilidades, errores u omisiones en la configuración de los Sistemas e infraestructura del Instituto FONACOT, que sean parte del "Servicio de detección e investigación de vulnerabilidades y pruebas de penetración", para mitigar el riesgo de fraude y así cumplir con los reglamentos internos y regulaciones que apliquen al Instituto FONACOT.

Prevenir ataques potenciales y simplificar el proceso de remediación.

El servicio deberá permitir la detección de vulnerabilidades en los sistemas internos y realizar el análisis de código de las aplicaciones críticas en El Instituto FONACOT para estar en condición de minimizar cualquier vulnerabilidad detectada.

La detección e investigación de vulnerabilidades deberá contemplar la infraestructura definida de común acuerdo entre El Instituto FONACOT y el LICITANTE en un plan de trabajo previamente establecido y deberá utilizar herramientas comerciales y no herramientas de libre distribución para la ejecución de este servicio.
Los componentes de la solución deberán estar integrados y gestionados por una única consola de administración con opciones de implementación en ambientes virtuales y físicos misma que será administrada por el especialista en ciber-amenazas.

8.2 Características del Servicio

8.2.1 El servicio deberá permitir obtener un nivel realista de riesgo y vulnerabilidades en contra de la tecnología, que comprenden las redes, aplicaciones, enrutadores, conmutadores, dispositivos, etc.
8.2.2 El servicio deberá realizar ataques múltiples que involucra varias facetas de pruebas de penetración, de aplicaciones, de la red y de los sistemas operativos.
8.2.3 El servicio deberá realizar diferentes pruebas con el objetivo de identificar las áreas de oportunidad, donde personas malintencionadas puedan comprometer todos los aspectos de la institución desde el acceso lógico a los sistemas y la información confidencial, que conduce a fuga de información y el compromiso de la red, los sistemas y daño reputacional.
8.2.4 El alcance del servicio constará de:

- Identificar vulnerabilidades de hardware, software y en la operación.
- Obtener una comprensión realista del riesgo para la institución y la posibilidad de materialización de los mismos.
- Ayudar a abordar y corregir todas las debilidades de seguridad identificadas.

8.2.5 El servicio deberá de llevarse a cabo consistentemente, utilizando marcos y estándar aceptados a nivel mundial y de la industria como OWASP, a fin de garantizar una operación sólida.

8.2.6 El servicio deberá tener una fase de pruebas para corroborar el nivel de seguridad actual de la institución, las cuales estarán divididas en las siguientes fases:

- Reconocimiento
- Explotación
- Acciones sobre el objetivo
- Análisis de resultados
- Recomendaciones y acciones de remediación

8.2.7 El LICITANTE deberá contar con un grupo de especialistas con experiencia táctica asignados para validar la seguridad de la institución en todo momento. Adicionalmente, el servicio deberá contemplar las siguientes actividades las cuales deberán de incluirse sin representar un costo extra para la institución:

- Evaluar la respuesta de la institución frente a los ataques externos.
- Mejorar y corregir los controles de seguridad implementados.
- Evaluar la solidez de la base de evidencia o la calidad de su información en el análisis de la información recabada durante el incidente.
- Prueba continua de la seguridad de sus sistemas, red y aplicaciones.
- Evaluar de forma periódica las medidas de seguridad implementadas y cómo se enfrentaría a las diferentes metodologías de ataque sin previa advertencia.

8.2.8 El servicio deberá utilizar una combinación de herramientas tecnológicas que se adecue al ecosistema del instituto, tales como:

- Nessus
- Rapid7
- SolardWins
- Acunetix Web Vulnerability Scanner
- Burp Suite
- Entre otras.

8.2.9 El servicio deberá contemplar la entrega de los resultados en un informe técnico detallado y un informe ejecutivo.

- Reporte técnico. - Informe que se realiza a nivel técnico detallado, que incluirá información sobre las vulnerabilidades identificadas, método de descubrimiento y forma de explotación, pasos para remediación.
- Reporte ejecutivo. - Informe ejecutivo debe de brindar una visión general del estado de la seguridad, con un enfoque de negocio donde se presentará el nivel general de riesgo, panorama general del análisis de riesgos identificados, recomendaciones generales y conclusiones.

8.3 Descripción de Componentes

8.3.1 Los servicios de detección e investigación de vulnerabilidades se deben de dar por lo menos dos veces al año.

8.3.2 En dado caso que la institución lo requiera más de dos veces al año, no deberá representar ningún costo adicional para el Instituto FONACOT.

8.3.3 Los artefactos contemplados en este esquema de solución deberán contener las características y especificaciones del soporte y pólizas de mantenimiento de los mismos.

8.4 Descripción de Funcionalidades

8.4.1 El servicio deberá contemplar un informe sobre los hallazgos de seguridad a nivel de sistema operativo, aplicaciones y bases de datos, e incluir las acciones requeridas para eliminar cada una de las vulnerabilidades identificadas. Además, dicho informa deberá destacar los riesgos de seguridad provenientes de los hallazgos y proporcionar una visión clara del nivel de seguridad de la organización.

8.4.2 El servicio de detección e investigación de vulnerabilidades deberá contemplar la infraestructura actual del instituto y el licitante, deberá generar un plan de trabajo en conjunto

con El Instituto FONACOT y se utilizarán herramientas comerciales para ejecutar este servicio, actualizadas y vigentes previo al análisis.

8.4.3 El servicio deberá contar con opciones de implementación en ambientes virtuales y físicos.

8.4.4 El servicio deberá soportar sistemas operativos Windows y Linux Red Hat y/o CentOS para su implementación.

8.4.5 El servicio deberá permitir la administración de los componentes a través de interfaces web, soportando los principales navegadores web, así como navegadores en tabletas o dispositivos móviles.

8.4.6 El servicio tendrá que ofrecer visibilidad continua sobre las posibles vulnerabilidades existentes dentro del instituto aun cuando no se estén ejecutando revisiones activas sobre la infraestructura.

8.4.7 El servicio deberá permitir el seguimiento de activos individuales a pesar de que su dirección IP cambie, ofreciendo métodos de detección que incluyan dirección IP, nombre de host, nombre DNS y dirección MAC.

8.4.8 El servicio deberá garantizar que toda la información resultante de las exploraciones de la infraestructura se transmita de forma segura entre todos los componentes del servicio y permanezcan dentro de las instalaciones del instituto en todo momento.

8.4.9 El servicio deberá asegurar la disponibilidad de los procesos y servicios del instituto ofreciendo:

- Mecanismos para controlar y evitar posibles impactos durante la realización de las exploraciones de vulnerabilidades.
- Programación recurrente de exploraciones, así como definición de fechas y horarios en los cuales en ninguna circunstancia se podrá realizar las exploraciones.

8.4.10 El servicio deberá ofrecer visibilidad sobre la postura de seguridad del instituto a través del tiempo, permitiendo observar las tendencias de presencia de vulnerabilidades y su tratamiento dentro del mismo.

8.4.11 El servicio deberá ofrecer al instituto la capacidad de configurar usuarios y grupos permitiéndole cumplir con el principio de separación de roles y responsabilidades, pudiendo autenticarlos ante los principales mecanismos de autenticación LDAP y Microsoft AD y limitando el acceso y la ejecución de acciones sobre listados particulares de activos.

8.4.12 El servicio deberá generar métricas sobre la cobertura de las líneas base de defensa de los activos, el cumplimiento del aseguramiento (hardening) de dispositivos o sistemas con respecto a estándares de la industria y la eficiencia de la aplicación de parches.

8.4.13 El servicio deberá generar un impacto mínimo en la red del instituto durante el proceso de escaneo.

8.4.14 El servicio deberá contar con un mecanismo para la realización de los análisis en forma rápida y se deberá considerar un balanceo de carga entre múltiples recursos (sensores) para descubrimiento y análisis de los dispositivos.

8.4.15 El servicio deberá de contar con la capacidad de hacer uso de la conexión directa con Microsoft Active Directory, para la creación de listas de activos conectados (estaciones de trabajo y servidores).

8.4.16 La solución deberá de ofrecer la siguiente información para las vulnerabilidades encontradas dentro del instituto:

a. Nombre
b. Nivel de riesgo (criticidad)
c. Descripción
d. Referencias
e. Recomendación (para la remediación)
f. Número de CVE(s) asociados

8.4.17 La solución deberá permitir el escaneo con credenciales y sin credenciales, así como contar con la utilización de mecanismos para elevar privilegios en caso de no tener una cuenta con privilegios de administración, como "root" en plataformas Unix y Linux.

8.4.18 La solución deberá contar con soporte para el desarrollo de scripts personalizados para el análisis de sistemas, dispositivos de comunicaciones y aplicativos instalados.

8.4.19 La solución tendrá que proporcionar plantillas predefinidas para el modelo ISO 27001.

8.4.20 La solución deberá de permitir la priorización de los escaneos, de modo que aquellos prioritarios puedan ejecutarse a toda velocidad, mientras que los demás se ejecuten más lentamente.

8.4.21 La solución deberá de ser capaz de conectarse con herramientas de escaneos pasivos y correlacionadores de eventos.

8.4.22 La solución deberá permitir especificar exclusiones para cada escaneo, para prevenir el escaneo de sistemas críticos.

8.4.23 La solución deberá de realizar escaneos con secuencias de comandos Web para detectar vulnerabilidades de las aplicaciones de servidor, tales como:

a. Microsoft Internet Information Server (IIS)
b. Apache
c. Java
d. JBoss
e. Tomcat

8.4.24 La solución deberá de permitir especificar el alcance de credenciales, limitando el acceso por medio de la dirección IP, el nombre del dispositivo, DNS, Nombre NetBIOS o listas de activos específicas.

8.4.25 La solución deberá de contar con la capacidad de elaborar reportes detallados que permitan clasificar las vulnerabilidades encontradas en el instituto de acuerdo con el riesgo asociado a cada una de éstas. Estos reportes deberán contar con las siguientes características:

- Correlacionar cada vulnerabilidad con la norma referencia.
- Permitir la personalización con las mismas secciones de un análisis de vulnerabilidad.
- Permitir la agrupación por equipo o responsable cada activo.
- Permitir configurar la ejecución de los escaneos por tiempos definidos (hora y minuto) y su frecuencia (diario, semanal, mensual).
- Proporcionar opciones avanzadas para permitir la categorización por unidad de negocio, bases de datos o rango de direcciones IP, con el fin de proporcionar visibilidad sobre violaciones de políticas, vulnerabilidades, acciones de remediación, y los cambios en los perfiles de riesgo del instituto.

8.4.26 La solución deberá proporcionar el análisis y mostrar los comentarios inmediatos a los desarrolladores sobre problemas y vulnerabilidades.

8.4.27 La solución deberá realizar verificación de seguridad a nivel de acceso.

8.4.28 La solución deberá hacer escaneos en el código en busca de vulnerabilidades.

8.4.29 La solución deberá permitir la administración de los accesos de los usuarios.

8.4.30 La solución deberá realizar análisis de código de diferentes lenguajes de programación.

8.4.31 La solución deberá permitir la verificación de compilación independiente.

8.4.32 La solución deberá tener la capacidad para integrarse con la infraestructura ya sea de forma local o remota.

8.4.33 La solución deberá tener la capacidad de responder ante aplicaciones críticas sin afectar el rendimiento.

8.4.34 La solución deberá contar con Independent Secure Build Verification.

9. SERVICIO DE CONTROL Y GESTIÓN DE USUARIOS.

9.1 Descripción del Servicio.

El servicio deberá asegurar el acceso a la infraestructura y sistemas informáticos del Instituto FONACOT. El LICITANTE deberá asignar a un ingeniero de validación de accesos de infraestructura tecnológica que gestione la solución tecnológica y asegure el control y supervisión a los accesos de los sistemas críticos del Instituto FONACOT, deberá robustecer el control de acceso, recabar y mantener evidencias en caso de cambios o modificaciones no autorizadas, así como garantizar que los usuarios cuenten con el acceso adecuado a los sistemas y aplicaciones de forma automatizada para evitar violaciones a la normatividad del Instituto y mantener la seguridad y el cumplimiento

de las políticas de seguridad. Deberá realizar aprovisionamiento, cambio de privilegios y baja de usuarios.

El servició deberá permitir el acceso controlado a los activos inherentes a los temas de seguridad de la información que integran el Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones, orquestar acciones de contención o prevención con tecnologías como firewall y escáner de vulnerabilidades entre otros. Realizar la administración de movilidad desde una única consola de administración centralizada que permita administrar la seguridad de las aplicaciones, los datos y la red.

9.2 Descripción de Componentes

9.2.1 La solución deberá permitir al menos los dispositivos que El Instituto FONACOT determine para la prestación del Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones, considerando el crecimiento que tenga la institución dentro del contrato.
9.2.2 La solución deberá permitir la administración mediante el Puerto serial.
9.2.3 La solución deberá tener 2 puertos USB, 2 back panel USB 2.0 + 1 front panel USB 2.0.
9.2.4 La solución deberá soportar hard drives.
9.2.5 La solución deberá soportar requisitos de enfriamiento de 2891 BTU/Hr.
9.2.6 La solución deberá permitir multi-Gbps de ancho de banda.
9.2.7 La solución deberá tener un consume de energía máximo de 744W.
9.2.8 La solución deberá contar con las entradas de VGA y CD-ROM.
9.2.9 La solución deberá contar al menos con la capacidad de interfaces de cobre y de fibra óptica de 1G y 10G.

9.3 Descripción de Funcionalidades

9.3.1 La solución del licitante deberá poder ser entregada en modalidad appliance físico o virtual, que incluya las licencias del sistema operativo y base de datos. Todos los componentes instalados y el sistema completamente configurado para su operación.
9.3.2 La solución del licitante deberá poder soportar modo activo/pasivo, para hacer la replicación de datos y alta disponibilidad
9.3.3 La solución del licitante deberá poder tener un appliance en un sitio alterno (físico o virtual) que pueda servir como recuperación de desastres (DRP)
9.3.4 La solución del licitante deberá poder soportar alta disponibilidad activo/activo nativamente para dividir las cargas entre los appliances y utilizar ambas plataformas simultáneamente
9.3.5 La solución del licitante deberá tener la capacidad de realizar un descubrimiento de información sobre contraseñas de activos de red trayendo los siguientes datos: última fecha de login, tipo de cuenta (privilegiada o estándar), grupo al que pertenece, si está habilitada o no y si la contraseña expira.
9.3.6 La solución del licitante deberá poder detectar automáticamente nuevas credenciales privilegiados de activos administrados de forma automática y hace cumplir la política de contraseñas para establecer estas nuevas credenciales
9.3.7 La solución del licitante deberá ser compatible con la gestión de cuentas privilegiadas con nombre, ejemplo "usuario", "usuario.admin" y "usuario_admin".
9.3.8 La solución del licitante deberá poder emitir informes DELTAS sobre el software, las cuentas de usuario instaladas identificados con el fin de conocer los cambios que se produjeron en cada servidor a través del tiempo
9.3.9 La solución del licitante deberá tener la capacidad de gestionar las cuentas con privilegios en los servidores con sistema operativo Windows Server 2008, 2008R2, 2012R2 y Server 2012
9.3.10 La solución del licitante deberá tener la capacidad de gestionar las cuentas con privilegios en los sistemas operativos para servidores Unix, Linux - Red Hat, SuSE, CentOS, Ubuntu, Debian, Solaris, etc.

9.3.11 La solución del licitante deberá tener la capacidad de gestionar las cuentas con privilegios en los sistemas de bases de datos Oracle, MySQL, MS-SQL

9.3.12 La solución del licitante deberá ser compatible con la gestión de las cuentas con privilegios para las aplicaciones Web como Facebook, Twitter, Instagram, LinkedIn, etc.

9.3.13 La solución del licitante deberá tener la capacidad de gestionar las cuentas con privilegios de activos de infraestructura de seguridad de la red

9.3.14 La solución del licitante deberá contar con un asistente para la creación de conectores para ejecutar el cambio de contraseña en plataformas que no están en la lista predeterminada

9.3.15 La solución del licitante deberá tener la funcionalidad para cambiar una contraseña de una cuenta en un servidor y pueda sincronizar la misma contraseña para la misma cuenta en otros servidores

9.3.16 La solución del licitante deberá tener un botón de "pánico", que cuando se identifica una incursión en un entorno particular (servidores web, por ejemplo), se puede hacer rápidamente un filtro en todos los servidores web y de inmediato hacer el cambio de contraseña para todas las cuentas privilegiadas de este entorno, a través de un solo clic

9.3.17 La solución del licitante deberá tener una herramienta de flujos de trabajo para la definición de aprobaciones para solicitar el acceso a las credenciales privilegiadas, con notificación a los aprobadores vía e-mail y la notificación por parte del interfaz de la herramienta

9.3.18 La solución del licitante deberá poder configurar un flujo de trabajo con el fin de tener dos o más aprobadores para liberar una contraseña

9.3.19 La solución del licitante deberá tener la posibilidad de permitir el acceso preautorizados

9.3.20 La solución del licitante deberá de poder configurar un flujo de trabajo sincronizado para la gestión de proveedores y terceros

9.3.21 6.1.21. La solución del licitante deberá ser compatible con la gestión automática de claves SSH (rotación de claves, flujo de trabajo de aprobación, etc.) para los usuarios que acceden servidores Linux o Unix a través de claves SSH y no utilicen la contraseña

9.3.22 La solución del licitante deberá soportar "passphrases" en la gestión de claves SSH

9.3.23 La solución del licitante deberá ofrecer conmutación para recuperación de clave a través de contraseñas en caso de problemas de conexión a través de llaves SSH

9.3.24 La solución del licitante deberá ser compatible con el cambio de contraseñas (rotación) en los archivos de configuración web.config

9.3.25 La solución del licitante deberá tener APIs para que las aplicaciones (Java, C, C ++, REST, etc.) puedan consumir las credenciales automáticamente en tiempo real, evitando que el usuario y la contraseña se expongan en el código fuente

9.3.26 La solución del licitante deberá poder un mecanismo propio de caché para permitir que miles de peticiones por segundo no afecten el rendimiento de las aplicaciones

9.3.27 La solución del licitante deberá permitir reproducir sesiones grabadas en la misma consola de gestión de contraseñas seguras

9.3.28 La solución del licitante deberá proporcionar una arquitectura basada en proxy para la gestión de cuentas privilegiadas, donde los usuarios se conectan a un punto central (portal web) y de este portal puede iniciar sesiones SSH, RDP, Web al servidor de destino con las cuentas protegidas por contraseñas seguras

9.3.29 La solución del licitante deberá ser compatible con una conexión transparente a los activos en cuestión, sin que el usuario puede ver e introducir la contraseña para realizar una conexión

9.3.30 La solución del licitante proporcionar la capacidad de soportar la conexión directa con el sistema Windows para los activos administrados

9.3.31 La solución del licitante deberá poder realizar la reproducción de vídeo, y con todo el acceso privilegiado que se lleva a cabo en un servidor específico

9.3.32 La solución del licitante deberá tener la funcionalidad de buscar entre las sesiones para identificar, por ejemplo, cuando en una sesión determinada se introdujo el nombre de la tabla "tarjetas" de una base de.datos

9.3.33 La solución del licitante deberá tener un campo para que los auditores ingresen sus comentarios después de la auditoría de una sesión especial para realizar un seguimiento de todas las sesiones grabadas, que en realidad están siendo auditados

9.3.34 La solución del licitante deberá poder delegar el acceso a una aplicación específica (por ejemplo, MS-SQL Studio, Oracle Developer, consola de administración de Checkpoint,

Facebook, etc.) a los usuarios, en lugar de dar una sesión completa de SSH o RDP en un servidor en particular

9.3.35 La solución del licitante deberá permitir realizar un seguimiento de una sesión activa en tiempo real, lo que permite la visualización de todos los comandos y aplicaciones en una sesión abierta por un usuario remoto para un acceso a una cuenta privilegiada

9.3.36 La solución del licitante deberá permitir a un administrador "pausar" o bloquear temporalmente una sesión sin afectar el trabajo usuario remoto De forma tal que pueda contener una cierta actividad presuntamente no autorizada, lo que permite tiempo para el análisis antes de decidir finaliza la sesión del usuario o desbloquear la sesión.

9.3.37 La solución deberá permitir a un usuario administrador terminar una sesión activa de forma remota.

9.3.38 La solución del licitante deberá tener un mecanismo para auditar las sesiones abiertas por "fuera" de la caja de seguridad en los servidores de Windows

9.3.39 La solución deberá tener mecanismo para auditar comandos privilegiados por "sudo" en Linux / Unix

9.3.40 La solución deberá tener mecanismos para identificar cuáles son las vulnerabilidades de cada activo en la organización, debido a su configuración o software

9.3.41 La solución del licitante deberá permitir la identificación de vulnerabilidades en Windows, Linux, Unix, Oracle, MS-SQL, dispositivos de red Cisco, Firewalls, Java, Adobe, etc.

9.3.42 La solución del licitante deberá tener la capacidad de realizar la correlación con exploits para identificar qué activos se pueden explorar fácilmente mediante herramientas de malware que ya están disponibles en el Internet

9.3.43 La solución del licitante deberá contener reportes que indican las acciones para remediación de vulnerabilidades, ya sea a través de parches y/o ajustes

9.3.44 La solución del licitante deberá permitir la instalación de parches para corregir automáticamente las vulnerabilidades en Windows, IE, Java, Adobe, Firefox, Chrome, Safari, SQL, etc., a través de la integración con la solución de gestión de parches

9.3.45 En la solución del licitante la función de administración de contraseñas de archivos de configuración (Web.config) y las contraseñas en el código fuente de las aplicaciones (Java, C, etc.) se podrán alojar por separado

9.3.46 La solución del licitante deberá proporcionar visibilidad mediante una combinación de técnicas de monitoreo activo y pasivo para descubrir dispositivos en el instante en que ingresan a la red, sin requerir agentes.

9.3.47 La solución deberá poder clasificar y evaluar dispositivos e instancias virtuales.

9.3.48 La solución deberá permitir monitorear continuamente los dispositivos a medida que entran y sales de la red.

9.3.49 La solución deberá poderse implementar fuera de banda en la red sin agregar latencia o un posible punto de falla de la red.

9.3.50 La solución deberá permitir, de manera enunciativa más no limitativa, rastrear y controlar usuarios, aplicaciones, procesos, puertos, dispositivos externos.

9.3.51 La solución deberá tener un motor de informes integrado que permita controlar el nivel de cumplimiento de políticas, cumplir con requisitos de auditorías.

9.3.52 La solución deberá tener la capacidad de crear informes de inventario en tiempo real

9.3.53 La solución deberá poderse implementar sin afectar a los usuarios o dispositivos

9.3.54 La solución deberá tener la capacidad de crear políticas de seguridad que se adecuen a los lineamientos del Instituto FONACOT

9.3.55 La solución deberá poder contar con plantillas, reglas e informes incorporados en las políticas, que permitan configurarse y administrarse

9.3.56 La solución del licitante deberá poder identificar, clasificar, autenticar y controla el acceso a la red sin un agente. Realice una inspección profunda del punto final sin un agente.

9.3.57 La solución deberá poder identificar automáticamente las infracciones de las políticas, remediar las deficiencias de seguridad de los puntos finales y medir el cumplimiento de lo reglamentado

9.3.58 La solución deberá poder detectar dispositivos sin direcciones IP, como dispositivos de captura de paquetes.

9.3.59 La solución deberá garantizar que las personas correctas con los dispositivos adecuados tengan acceso a los recursos de red apropiados
9.3.60 La solución deberá resolver infracciones de bajo riesgo enviando un aviso al usuario final o solucionando automáticamente el problema de seguridad; permitiendo que el usuario siga operando mientras ocurre la reparación
9.3.61 La solución deberá poder utilizar 802.1X u otras tecnologías de autenticación como LDAP, Active Directory, RADIUS, Oracle y Sun.
9.3.62 Los artefactos contemplados en este esquema de solución deberán contener las características y especificaciones del soporte y pólizas de mantenimiento de los mismos.

10. SERVICIO DE PROTECCIÓN DE BASES DE DATOS.

10.1 Descripción del Servicio

Implementar un esquema de fortalecimiento de seguridad informática, que evite que los datos en reposo sean explotados por aplicaciones o usuarios no autorizados. El LICITANTE deberá asignar un especialista en seguridad en sistemas operativos que será el responsable de gestionar la solución encargada de monitorizar, bloquear y alertar en tiempo real la actividad de los usuarios en las bases de datos del Instituto FONACOT y registrar la actividad de los usuarios y reportar las actividades relevantes que sean identificadas, así mismo, deberá implementar mecanismos de seguridad que permitan la protección de la información almacenada en las bases de datos ante posibles filtraciones de información que comprometan la información propiedad del Instituto FONACOT.

10.2 Descripción de Componentes

10.2.1 La solución deberá tener una capacidad mínima operativa por appliance de 500/1000/2000/5000/10000 Mbps de tráfico inspeccionado.
10.2.2 La solución deberá soportar opciones de conectividad física como 1Gb Ethernet en UTP o Fibra Óptica tipo SX, así como conectividad 10Gb en modos SR o LR.
10.2.3 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 appliance.
10.2.4 La solución deberá soportar el volumen de tráfico y deberá tener una latencia menor a 5ms, para no impactar el desempeño de las aplicaciones.
10.2.5 La solución deberá tener al menos 1 GB de throughput.
10.2.6 La solución deberá tener de memoria al menos 30 GB DDR3.
10.2.7 La solución deberá tener de almacenamiento en disco duro 2 TB.
10.2.8 La solución deberá contar con SSL Acceleration.
10.2.9 La solución deberá contar con Puerto serial, Puerto USB, Out-of-Band Port Management, Puerto IMPI.
10.2.10 La solución deberá contar con unidades de disco duro duales intercambiables (hot-swap).
10.2.11 La solución deberá mantener una latencia de <5ms.
10.2.12 La solución deberá contar al menos con 5 segmentos de red.
10.2.13 Cada consola de la solución propuesta deberá tener la capacidad de soportar un crecimiento para la gestión de agentes. El número de agentes se definirá con base en los requerimientos del Instituto FONACOT.
10.2.14 Todos los elementos de la solución propuesta deben ser de la misma marca y fabricante.
10.2.15 La solución deberá tener como mínimo 12 GB de memoria.
10.2.16 La solución deberá contar con 1 puerto serial, 2 interfaces de ethernet x 1GB, puerto IMPI de 1x10/100MB.

10.3 Descripción de Funcionalidades

10.3.1 La solución deberá contar con tecnología de autoaprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos,

incluyendo schemas, objetos, tablas; sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario; todo esto para el establecimiento de un baseline de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.

10.3.2 La solución deberá proporcionar protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.

10.3.3 La solución deberá soportar ser desplegada o implementada en línea como un puente o bridge transparente (capa 2 del Modelo OSI, las interfaces no requieren de una dirección IP y debe soportar bypass/ failopen/ failclose configurable tanto para fallas de hardware como software), como un proxy transparente o un proxy inverso (según se requiera), o como un analizador no en línea o un non-inline sniffer / monitor, a través de puertos Mirror o SPAN.
Deberá también:

- 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, la solución deberá bloquear ataques proactivamente.
- Respecto de algún ataque o alguna otra actividad no autorizada, la solución 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, la solución deberá ser capaz de bloquear la dirección IP por un periodo de tiempo configurable.
- En modo analizador de paquetes o sniffer, la solución deberá ser capaz de enviar un paquete TCP RST a ambos extremos de la conexión. Alternativamente, si así se configura, la solución podrá reportar el comportamiento anómalo, pero no tomar acción alguna.

10.3.4 La solución deberá generar reportes y tendencias en tiempo real, así como permitir la modificación de los mismos.

10.3.5 La solución deberá contar con facilidades o herramientas analíticas para la conducción de análisis forense cuando sea reportado algún incidente

10.3.6 La solución no deberá requerir el instalar agentes de software en los servidores a monitorear, pero deberá tener la opción en caso de ser necesario.

10.3.7 La solución deberá funcionar independiente a la activación de la auditoría nativa de la base de datos.

10.3.8 La solución deberá ser transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.

10.3.9 El repositorio para el registro de la actividad en el appliance, 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.

10.3.10 La solución deberá ser capaz de descubrir servidores de bases de datos y realizar detección e investigación 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.

10.3.11 La solución deberá realizar una evaluación exhaustiva de los riesgos de la infraestructura objetivo a diferentes niveles/capas de la infraestructura de base de datos incluyendo:

- Cuestiones 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.
- Cuestiones de configuración de la plataforma, incluyendo configuración del sistema operativo de los servidores que soportan el software de base de datos.

10.3.12 La solución deberá de 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.

10.3.13 La solución deberá 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.

10.3.14 La solución deberá 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.

10.3.15 La solución deberá apoyar en los esfuerzos de detección e investigación de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y Control de cambios.

10.3.16 La solución deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.

10.3.17 La solución deberá monitorear e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, ligas, stored procedures, entre otros.

10.3.18 La solución deberá hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.

10.3.19 La solución deberá proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.

10.3.20 La solución deberá manejar reglas y políticas tan amplias o granulares como se requieran y deberán poder ser construidas automáticamente o manualmente y deberán poder ser actualizadas, igualmente, de forma manual o automática.

10.3.21 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:

- Por operaciones básicas (Select, Insert, Update, Delete)
- Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export)
- Tipo de datos accesado (financiero, recursos humanos, inventarios, o cualquier definición personalizada)
- Acceso a datos marcados como sensibles
- Base de Datos, Schema, Tabla y Columna accesada
- Estado de autenticación de la sesión
- Usuario y/o Grupo de Usuarios de Base de Datos conectado
- Usuario conectado en la capa aplicativa, a diferencia del usuario conectado a la DB
- Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier adaptación por expresiones regulares)
- Logins, Logouts, Queries
- IPs de origen y destino
- Número de registros a regresar por la consulta (SQL Query)
- Número de registros afectados
- Número de ocurrencias en intervalos de tiempo definidos
- Nombre de Host origen, Usuario firmado en el Host origen
- Aplicación usada para la conexión a la base de datos
- Tiempo de respuesta/procesamiento del query
- Errores en el manejador de SQL
- Por Stored Procedure o Function utilizada
- Si existe ticket asignado de cambios
- Horario

10.3.22 La solución deberá identificar individualmente a los usuarios finales que realicen actividades mediante aplicaciones, 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.

10.3.23 Debe posibilitar los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.

10.3.24 La solución deberá asociar y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son indicativos de una potencial violación de seguridad.

10.3.25 La solución deberá proteger contra ataques SQL y no-SQL (como buffer overflow).

10.3.26 La solución deberá correlacionar actividad en base de datos con actividad de aplicaciones web para entender detalladamente como los usuarios están accediendo datos privilegiados sin necesidad de alterar la aplicación web.

10.3.27 Considerados de emergencia para potenciales violaciones de la información que incluyan, enunciativa mas no limitativamente:

- Altos volúmenes de acceso a datos sensibles más allá de lo habitual.
- Acceso a datos inusual para cierta hora del día.
- Acceso a datos desde una ubicación desconocida.
- Acceso a datos utilizando aplicaciones/herramientas no autorizadas.

10.3.28 Debe manejar una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.

10.3.29 Debe tener facilidades de Archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP).

10.3.30 La solución deberá contar con Políticas, Reportes, Alertas, Objetos Sensibles, y Transacciones preidentificadas y preconfiguradas para trabajar con las plataformas empresariales del Instituto FONACOT.

10.3.31 La solución deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.

10.3.32 La solución deberá analizar los eventos generados desde diferentes bases de datos. El análisis deberá contemplar los siguientes criterios:

- Deberá mostrar el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos.
- Deberá contar con un sistema de correlación basado en la dirección de los ataques. Deberá determinar si los ataques provienen desde dentro de la organización hacia afuera de la misma o viceversa.
- Deberá realizar una correlación automática y en tiempo real de eventos, vulnerabilidades y bases de datos.
- Deberá ejecutar una correlación que permita identificar usuarios de aplicación asociados con consultas –y determinadas actividades– en bases de datos específicas sin necesidad de alterar aplicaciones o instalar API's.
- Deberá correlacionar eventos como número de errores inusuales de sentencias de SQL o al momento de hacer login a las bases de datos.

10.3.33 Debe permitir el manejo de alarmas y notificaciones –en tiempo real– para los eventos de correlación mencionados anteriormente.

10.3.34 Debe tener la capacidad de monitorear aplicaciones web en la misma solución, ofreciendo una visibilidad, seguridad y control desde el usuario web hasta la base de datos.

10.3.35 La solución deberá contar con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de las mismas.

10.3.36 La solución deberá soportar y aplicar simultáneamente un modelo de seguridad positivo y negativo.

10.3.37 El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que deberá además cumplir con las siguientes especificaciones:

- Deberá bloquear las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
- Deberá incluir una lista pre configurada y detallada de las firmas de ataque.
- Deberá permitir la modificación o adición de firmas por el administrador.
- Deberá permitir la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.

- Deberá detectar ataques conocidos en múltiples niveles, incluyendo, la red, sistemas operativos, software del servidor web y ataques a nivel de aplicación.

10.3.38 La solución deberá soportar Gateway clúster a nivel de los agentes de monitoreo de Bases de Datos, es decir que los agentes estarán asignados a un Gateway y podrán moverse automáticamente o manualmente según sea el caso sin necesidad de volver a registrar el agente con el Gateway 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.

10.3.39 Debe proporcionar un proceso de instalación, actualización y gestión de cambios centralizada, segura y ágil para los Agentes; la cual debe proporcionar una visión completa de todas las actualizaciones disponibles para los componentes de la solución de protección de Bases de Datos.

10.3.40 La solución deberá notificar cuando se encuentre disponible una nueva versión de Agente.

10.3.41 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.

10.3.42 La solución deberá proporcionar información del tráfico enviado de los Agentes a los Gateways, 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.

10.3.43 La solución deberá contar con la opción de reducir el tráfico entre la comunicación entre el Agente y el Gateway utilizando métodos de comprensión de datos.

10.3.44 La solución deberá proporcionar la opción de enmascarar la información personal que se despliega atreves de la interfaz de administración, además deberá contar con la opción de desenmascarar esta información dependiendo los privilegios de cada usuario.

10.3.45 Los artefactos contemplados en este esquema de solución deberán contener las características y especificaciones del soporte y pólizas de mantenimiento de los mismos

11. SERVICIO DE ADMINISTRACIÓN DEL MGSI.

11.1 Descripción del Servicio.

El LICITANTE mediante el personal en sitio deberá identificar los principales activos de información y realizar una evaluación de riesgos de los principales activos de información y su valoración a nivel cualitativo o cuantitativo.

EL LICITANTE deberá considerar las siguientes actividades como alcance del Servicio:

El LICITANTE mediante el personal en sitio 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", 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:

- Estándares Técnicos emitidos por la Coordinación de Estrategia Digital Nacional (CEDN).
- 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.
- Identificación y revisión de los controles de seguridad requeridos por la Coordinación de Estrategia Digital Nacional (CEDN).

El LICITANTE deberá establecer y/o fortalecer los controles adecuados de seguridad de la información a través de los controles seleccionados e indicadores para la medición efectiva de los controles.

11.2 Características del Servicio

11.2.1 El LICITANTE adjudicado deberá identificar los procesos y activos esenciales del Instituto FONACOT.

11.2.2 El LICITANTE adjudicado deberá elaborar un análisis de riesgos que permita evaluar e identificar los requisitos de seguridad de la institución, definiendo las potenciales amenazas a los activos asociados a los procesos estratégico de la Institución y a los activos de información del Instituto FONACOT, su vulnerabilidad, la probabilidad de ocurrencia y su posible impacto. 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.

11.2.3 El licitante ganador deberá elaborar el Plan de Seguridad de la Información tomando en consideración tanto los riesgos y niveles de servicio de la institución, así como las brechas existentes en temas de seguridad. Con base a este plan se definirán los controles necesarios que aseguren la reducción de los riesgos identificados, para cubrir en forma adecuada las necesidades específicas de la institución.

11.2.4 El LICITANTE deberá realizar ejercicio de medición de controles que puedan afectar la seguridad de la información, con la finalidad de comprobar su eficacia.

11.2.5 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.

12. REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN.

El Licitante ganador deberá contemplar como parte inherente de los servicios el realizar los análisis forenses de incidentes de seguridad que el Instituto FONACOT requiera durante la toda vigencia del contrato sin que estos generen un costo adicional al Instituto FONACOT. El licitante ganador deberá realizar a petición del Instituto FONACOT, el análisis de cómputo forense que incluye: la documentación, la gestión del dispositivo, el análisis de la imagen forense, la elaboración, revisión y presentación del informe forense con los resultados del análisis; todo con el fin de dar claridad y

sustento sobre los posibles incidentes de seguridad de la información que el Instituto FONACOT sufra, debido entre otras causas, a actividades realizadas por los usuarios a través de los servicios tecnológicos proporcionados por el Instituto FONACOT .

A su vez como parte del Análisis Forense, el Licitante ganador deberá realizar un análisis previo para entender el evento ocurrido mediante una reunión de contextualización con personal del Instituto FONACOT, en la cual proporcionará la información que posea al respecto, facilitando acceso a las fuentes relevantes de información y será el responsable del embalaje y resguardo físico del dispositivo de cómputo relacionado.

Una vez realizado esto el licitante:

- Deberá hacer la colección y preservación de la imagen forense.
- Deberá llevar a cabo el análisis de cómputo forense incluyendo las líneas de tiempo asociadas y la correlación de eventos propia de la investigación.
- Al finalizar realizará la presentación ejecutiva del informe y hará la resolución de dudas de modo presencial.
- Para fines legales el Instituto FONACOT designará entre su personal al responsable para presentar el documento ante las instancias legales que así le convengan.
- La solución propuesta por el licitante para brindar el Análisis Forense, deberá contar con las siguientes funcionalidades y será realizado utilizando herramientas especializadas tales como:
    i. Artefactos tecnológicos de análisis forense reconocidas por la industria.
    ii. Herramientas para el análisis y procesamiento de archivos de texto.
    iii. Herramientas de software para el análisis de volcados de memoria.

A continuación, se describen la documentación que deberá de entregar el licitante ganador al Instituto FONACOT cada vez que requiera este servicio como parte de los análisis forenses:

NOMBRE	DESCRIPCIÓN	PERIODICIDAD
SOW	Documento Statement of Work que describe los alcances (lista de aplicaciones a analizar indicada por el IFT), premisas y consideraciones, actividades y responsables para la entrega y aceptación del servicio de cómputo forense.	Por evento de análisis solicitado
INFORME DE ANÁLISIS DE CÓMPUTO FORENSE - TÉCNICO	Documento que detalla las técnicas utilizadas para realizar el análisis forense. Lista las herramientas utilizadas para la atención del caso, contiene el sustento en materia tecnológica de lo descrito sobre los hallazgos e indicios identificados.	Por evento de análisis solicitado
COPIA DE LAS IMÁGENES FORENSES ADQUIRIDAS (COPIAS BIT A BIT)	Copia exacta bit a bit de todos los datos digitales (evidencia digital) conforme o de acuerdo con cada dispositivo electrónico adquirido; realizada de una manera que garantiza que la información no sea alterada. La entrega de dicha información deberá de realizarse de forma cifrada-.	Por evento de análisis solicitado
MEMORIA TÉCNICA DE ADQUISICIÓN DE INFORMACIÓN	Documento que detalla física y lógicamente los indicios de los que se colectarán las imágenes forenses.	Por evento de análisis solicitado

El licitante deberá considerar, si el Instituto FONACOT así lo requiere, que previo a la puesta en operación de cada herramienta de seguridad, se lleve a cabo un análisis de vulnerabilidades, el cual podrá solicitarse al licitante y se deberá realizar a través de un tercero, sin generar esto un costo

adicional para el Instituto FONACOT. El resultado del análisis deberá preservarse para efectos de auditoría.

13. ADMINISTRACIÓN DE LOS SERVICIOS.

El licitante ganador deberá contar con la cantidad del personal técnico y administrativo referenciado dentro del presente documento que sean necesarios para cumplir con los planes de trabajo programados definidos por el Administrados del proyecto del Licitante y que abarcan la instalación, puesta en marcha y operación del SERVICIO INTEGRAL DE FORTALECIMIENTO EN LA GESTIÓN, ADMINISTRACIÓN Y CONTROL DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES.

El licitante ganador deberá asegurar la correcta implementación de todas las soluciones tecnológicas a través del personal cuyo rol está plasmado como "10 Personal en Sitio" (renglón no. 14 de la siguiente tabla), y que de manera simultánea aseguren la correcta implementación y transición de los servicios inherentes al presente Anexo Técnico.

Asimismo, el licitante deberá considerar la siguiente plantilla mínima de personal en su propuesta de servicio integral.

No.	PLANTILLA DE PERSONAL				
	Cantidad Mínima a Presentar.	Rol	C.V con los siguientes años de experiencia mínimos en proyectos similares	Estudios Académicos Se comprobara a través del acceso del portal/cliente/sitio de los documentos correspondientes, por lo tanto, deberá plasmar la información respectiva para esta verificación (URL, CLAVES, PASSWORD, NOMBRE DE USUARIO, por mencionar algunos).	Certificaciones Se comprobará a través del acceso del portal del emisor de los documentos correspondientes, por lo tanto, deberá plasmar la información respectiva para esta verificación (URL, CLAVES, PASSWORD, NOMBRE DE USUARIO, por mencionar algunos).
1	1	Especialista en gestión de servicios y seguridad de la información.	5	Cédula o título profesional a nivel Licenciatura de carreras tales como: Sistemas Computacionales, Informática, Telecomunicaciones, Electrónica o afines a las actividades del proyecto.	• GIAC Continuous Monitoring Certification (GMON). y/o • EC-Council Ethical Hacker;
2	1	Especialista en ciber-amenazas.	5	Cédula o título profesional a nivel Licenciatura de carreras tales como: Sistemas Computacionales, Informática, Telecomunicaciones, Electrónica o afines a las actividades del proyecto.	• CISA Certified Information Systems Auditor. y/o • CISM Certified Information Security Manager. y/o • CRISC Certified in Risk and Information Systems Control
3	1	Ingeniero de validación de accesos de infraestructura tecnológica.	5	Cédula o título profesional a nivel Licenciatura de carreras tales como: Sistemas Computacionales, Informática, Telecomunicaciones, Electrónica o afines a las actividades del proyecto.	• CCNA Certified Network Associate Routing and Switching. y/o • Certificación en Secure Access

No.	PLANTILLA DE PERSONAL				
	Cantidad Mínima a Presentar	Rol	C.V con los siguientes años de experiencia mínimos en proyectos similares.	Estudios Académicos. Se comprobará a través del acceso del portal del emisor de los documentos correspondientes, por lo tanto, deberá plasmar la información respectiva para esta verificación. (URL, CLAVES, PASSWORD, NOMBRE DE USUARIO, por mencionar algunos)	Certificaciones. Se comprobará a través del acceso del portal del emisor de los documentos correspondientes, por lo tanto, deberá plasmar la información respectiva para esta verificación. (URL, CLAVES, PASSWORD, NOMBRE DE USUARIO, por mencionar algunos)
4	1	Especialista en seguridad de sistemas operativos	5	Cédula o título profesional a nivel Licenciatura de carreras tales como: Sistemas Computacionales, Informática, Telecomunicaciones, Electrónica o afines a las actividades del proyecto.	• ITIL Certificate in IT service management y/o • GICSP Global Industry Cyber Security Professional
5	1	CyberSecurity Leader.	3	Cédula o título profesional a nivel Licenciatura de carreras tales como: Sistemas Computacionales, Informática, Telecomunicaciones, Electrónica o afines a las actividades del proyecto.	• CISSP Certified Information Systems Security Professional. y/o • Certified ISO/IEC 27001 Lead Implementer. y/o • Cobit 5 Foundation y/o • ITIL versión 3 foundation Examination.
6	1	Specialist Incident Handler	1	Cédula o título profesional a nivel Licenciatura de carreras tales como: Sistemas Computacionales, Informática, Telecomunicaciones, Electrónica o afines a las actividades del proyecto.	• Certificado vigente como especialista en alguna solución de validación de identidad que tenga base instalada dentro de una dependencia de gobierno.
7	1	Ingeniero en investigación de vulnerabilidades y pentesting	3	Cédula o título profesional a nivel Licenciatura de carreras tales como: Sistemas Computacionales, Informática, Telecomunicaciones, Electrónica o afines a las actividades del proyecto.	• Certificación en alguna herramienta comercial de Análisis de Vulnerabilidades. como, por ejemplo: • Tenable • Acunetix Etc
8	1	Administrador del Proyecto Especialista en Seguridad.	1	Cédula o título profesional a nivel Licenciatura de carreras tales como: Sistemas Computacionales, Informática, Telecomunicaciones, Electrónica o afines a las actividades del proyecto.	• Project Magnament Professional y/o • ISO IEC 27001 information security associate y • ITIL V4 Foundation Certificate
9	1	Especialista en validación de identidad	2	Cédula profesional a nivel licenciatura de carreras tales como: Sistemas Computacionales, Informática, Telecomunicaciones, Electrónica o afines a las actividades del proyecto.	• CISSP Certified Information Systems Security Professional. y/o • Certified ISO/IEC 27001 Lead Implementer. y/o • Cobit 5 Foundation y/o • ITIL versión 3 foundation Examination.

No	PLANTILLA DE PERSONAL				
	Cantidad Mínima a Presentar	Rol	C V con los siguientes años de experiencia mínimos en proyectos similares	Estudios Académicos Se comprobará a través del acceso del portal del emisor de los documentos correspondientes, por lo tanto, deberá plasmar la información respectiva para esta verificación. (URL, CLAVES, PASSWORD, NOMBRE DE USUARIO, por mencionar algunos)	Certificaciones Se comprobará a través del acceso del portal del emisor de los documentos correspondientes, por lo tanto, deberá plasmar la información respectiva para esta verificación. (URL, CLAVES, PASSWORD, NOMBRE DE USUARIO, por mencionar algunos)
10	1	Administrador del Proyecto.	3	Cédula o título profesional a nivel Licenciatura de carreras tales como: Sistemas Computacionales, Informática, Telecomunicaciones, Electrónica o afines a las actividades del proyecto.	• Project Magnament Professional y/o • ISO IEC 27001 information security associate y/o ITIL V4 Foundation Certificate
11	11				

14. REEMPLAZO DE PERSONAL

En caso de que se requiera sustituir algún miembro del equipo por parte del licitante a causa de desconocimiento de las plataformas de seguridad, deficiencias en el desempeño, mala conducta, entre otras, éste deberá de ser reemplazado, en un lapso no mayor a 3 (tres) días hábiles, por personal que cumpla con los perfiles solicitados con la experiencia, a fin de que no se pierda la continuidad en el trabajo desempeñado. Para el demás personal que se requiera sustituir del equipo de trabajo, el licitante ganador contará hasta con 5 (cinco) días hábiles para su sustitución. Será responsabilidad del Licitante ganador involucrar al nuevo integrante, así como de ponerlo al tanto del estatus del proyecto.

Es responsabilidad del Licitante tener la capacidad del personal en sitio para atender picos de demanda de servicios de emergencia de 24x7x365. En caso de incumplimiento se aplicará la deductiva correspondiente. Los picos de demanda deberán atenderse a nivel nacional sin incurrir en costes adicionales para el Instituto Fonacot y durante toda la vigencia del contrato.

En cualquier evento de sustitución del personal del Licitante ganador, se deberá entregar a la Subdirección General de Tecnologías de la Información y Comunicación, carta firmada por el representante legal indicando el motivo de la sustitución. La Subdirección General de Tecnologías de la Información y Comunicación, se reserva el derecho de solicitar la documentación que avale la experiencia.

El licitante ganador no podrá sustituir a más del 30% del personal por proyecto a menos que sea a solicitud de la Subdirección General de Tecnologías de la Información y Comunicación.

15. ESTÁNDARES.

El Instituto FONACOT tiene definidos estándares (se entregarán al Licitante ganador) que se deben considerar en todos los proyectos.

El licitante deberá apegarse a los lineamientos que establece el ACUERDO por el que se expide la Estrategia Digital Nacional 2021-2024, en materia de tecnologías de la información y comunicaciones y 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; ambos publicados en el Diario Oficial de la Federación el 06 de septiembre de 2021.

16. GARANTÍA DE CALIDAD DE LOS SERVICIOS.

El servicio que el Instituto FONACOT requiere durante el periodo de garantía de calidad de los servicios, se refiere a la corrección de errores como consecuencia de la implementación de las herramientas de seguridad de la información o herramientas de monitoreo para la seguridad de la información, que pudieran aparecer una vez implementados las herramientas propuestas para la solución del servicio integral, considerando los niveles de servicio especificados en este numeral y con cargo al licitante ganador.

El licitante ganador, al terminar cada servicio integral mensual de: mantenimiento, soporte u operación de productos o servicios inherentes al presente, deberá presentar una carta compromiso a la Subdirección General de Tecnologías de la Información y Comunicación, donde garantice:

16.1 Solución de defectos.

Solucionar cualquier defecto por concepto del servicio o producto prestado cuestión de este Anexo Técnico.

16.2 Mal entendimiento.

Que las modificaciones a la plataforma tecnológica causadas por un mal entendimiento del análisis (Se entiende por mal entendimiento del análisis a todo lo que no corresponda a la funcionalidad descrita y aceptada por la Subdirección General de Tecnologías de la Información y Comunicación), o errores en la operación o fallas de ejecución, deberán ser cubiertas por el licitante ganador sin cargo a las horas inicialmente pactadas ni costo adicional para el Instituto FONACOT.

16.3 Atención de Fallas.

El licitante deberá documentar el mecanismo para la atención de incidentes.

16.4 Levantamiento de garantías.

El licitante deberá presentar dentro de su propuesta una carta firmada por el representante legal, donde se comprometa a proporcionar contacto, dirección electrónica, número telefónico y matriz de escalamiento para el levantamiento de garantías.

16.5 Atención a Garantías.

La solicitud podrá realizarse vía telefónica, por correo electrónico o de manera escrita al director de Proyectos del licitante ganador (se confirmará vía correo electrónico y telefónico), describiendo el problema encontrado y el nivel de severidad, para que el licitante ganador cumpla con los siguientes tiempos requeridos por el Instituto FONACOT:

No.	Descripción	Tiempo máximo de Respuesta	Tiempo máximo de Solución
1	El sistema no puede operar o alguno de sus módulos impide que el proceso siga su marcha.	30 min.	2 horas
2	El sistema mostró una falla grave, pero se puede seguir operando y no se detiene la operación.	1 hora.	8 horas
3	El sistema tiene problemas mínimos que no detiene ni afectan la operación del mismo.	2 horas.	24 horas

16.6 Vigencia de la garantía.

La garantía será durante toda la vigencia del contrato desde la adjudicación y hasta la fecha en la que la Subdirección General de Tecnologías de la Información y Comunicación, firme la carta de entrega-recepción del servicio o producto, la cual marca el final de este, y cuyo formato y contenido será proporcionado por la Subdirección General de Tecnologías de la Información y Comunicación.

17. GARANTIZAR LOS NIVELES DE SERVICIO (SLA´s)

17.1 Requerimientos mínimos para garantizar los SLA's.

a. El Instituto FONACOT podrá solicitar la presencia de cualquier recurso humano asignado a los servicios objeto de esta licitación, la cual deberá presentarse en la Subdirección General de Tecnologías de la Información y Comunicación máximo en 1 (una) horas, por lo que las instalaciones de las oficinas administrativas del licitante participante deberán estar ubicadas en un radio no mayor a los 20 kilómetros del edificio sede del **INSTITUTO FONACOT.**
b. La comunicación verbal y escrita deberá ser invariablemente en español de México, salvo en aquellos tecnicismos que no tengan una traducción clara.

17.2 Mesa de servicio.

Interface de la mesa de ayuda del licitante ganador con la Mesa de Servicios del **Instituto FONACOT** para el control y administración de las incidencias.

18. VIGENCIA, LUGAR Y HORARIO DE LA PRESTACIÓN DEL SERVICIO.

a. **Vigencia**.
El contrato que se derive del presente procedimiento tendrá una vigencia del 16 de agosto del 2022 al 31 de diciembre de 2022.

De conformidad con lo establecido en el quinto párrafo del artículo 84 del REGLAMENTO DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO, la prestación del servicio se llevará a cabo de conformidad con lo solicitado en el Anexo, sin prejuicio de que se cumpla con la obligación de formalizar el contrato dentro del plazo establecido.

b. **Horario**.
Para la entrega de los servicios se apegarán a los horarios laborales del Instituto FONACOT, sin perder de vista, horarios atípicos, de acuerdo a la complejidad y/o prioridad de los proyectos previa solicitud de la Subdirección General de Tecnologías de la Información y Comunicación
En la planeación de los planes de trabajo detallados para los proyectos, solo se deberán contabilizar hasta 8 horas diarias por recurso humano, no siendo limitativo las horas presenciales por atrasos en la entrega de los trabajos encomendados o cargas de trabajo atípicas derivadas de la operación del Instituto FONACOT.

c. Lugar
El Administrador del Proyecto, Personal en Sitio, y el Especialista en Seguridad del licitante ganador deberán de prestar sus servicios en el edificio sede del Instituto FONACOT, sita en Avenida Insurgentes Sur No. 452, Colonia Roma Sur, Delegación Cuauhtémoc, CP. 06760, Ciudad de México, de acuerdo a las necesidades de la Convocante, el resto del personal deberá de prestar sus servicios en las oficinas del licitante ganador, sin embargo, deberán presentarse cuando así lo requiera el Instituto

FONACOT, en un tiempo no mayor a 1 (una) hora en las instalaciones de la misma a partir de la notificación que será por correo electrónico.

Asimismo, y de ser el caso, prestará el servicio en las oficinas y sucursales del Instituto FONACOT sin costo alguno, de acuerdo con las necesidades del servicio previa notificación con 8 horas por parte de la Subdirección General de Tecnologías de la Información y Comunicación, cuyos domicilios se presentan a continuación:

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.

Región	Nombre de Sucursal	Domicilio
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, C.P. 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.

Región	Nombre de Sucursal	Domicilio
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.
		Calle Venustiano Carranza No. 410, locales 2, 3 y
Norte	Monclova	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.

Región	Nombre de Sucursal	Domicilio
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,
Norte	Cabo San Lucas	C.P. 23920, Santa Rosalía, Mulege, Baja California Sur. (Oficina Conapesca y SAGARPA) 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.

Región	Nombre de Sucursal	Domicilio
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.

Región	Nombre de Sucursal	Domicilio
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	Jesús Carranza No 213 Local 201, col. Centro C.P 90300, Apizaco, Tlaxcala

19. PLAZO PARA LA SUSPENSIÓN DEL SERVICIO.

El plazo para la suspensión del servicio será de 10 días hábiles. Asimismo, la suspensión de la prestación de los servicios se ajustará a lo dispuesto por los artículos 55 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 102 fracción II de su Reglamento.

20. FORMA DE PAGO

Con fundamento en el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el pago se realizará en pagos mensuales, o de acuerdo con los servicios devengados debidamente soportado y acompañado con los entregables que apliquen de acuerdo al numeral **"22. ENTREGABLES"**, del presente Anexo Técnico.

El pago se realizará dentro de los 20 días naturales posteriores a la presentación del Comprobante Fiscal Digital por Internet CFDI (factura electrónica impresa y archivo XLM) y previa validación y aceptación de la misma, por parte de la Subdirección General de Tecnologías de la Información y Comunicación y recibidos los entregables mencionados anteriormente a entera satisfacción de la Subdirección General de Tecnologías de la Información y Comunicación.

Los CFDI's (facturas) deberán contar con el visto bueno de la Subdirección General de Tecnologías de la Información y Comunicación y del titular de la DTI, 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. Dichos comprobantes serán entregados en las oficinas centrales del Instituto FONACOT, ubicadas en Avenida Insurgentes Sur No. 452, 2° Piso, Col. Roma Sur, C.P. 06760, Delegación Cuauhtémoc, Ciudad de México, en la **Subdirección General de Tecnologías de la Información y Comunicaciones**, así mismo deberán ser enviados al correo electrónico a horacio.sanchez@fonacot.gob.mx, en un horario de labores de las 9:00 a las 15:00 horas de lunes a viernes en días hábiles.

El pago, quedará condicionado, proporcionalmente, al pago y/o deducción que el prestador de servicio deba efectuar por concepto de penas convencionales.

Tratándose de pagos en exceso que haya recibido el licitante ganador, se deberá reintegrar la cantidad pagada en exceso, más los intereses correspondientes, conforme a la tasa que será igual a la establecida por la Ley de Ingresos de la Federación. En los casos de prórroga para el pago de Créditos Fiscales, los recargos se calcularán sobre las cantidades pagadas en exceso en cada caso y se computarán por días naturales desde la fecha del pago, hasta la fecha en que se pongan efectivamente las cantidades a disposición del Instituto FONACOT, de conformidad con lo establecido en el artículo 51, párrafo tercero y cuarto de la LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO.

En caso de que el licitante ganador presente sus facturas con errores o deficiencias, el plazo de pago se ajustará en términos de los artículos 89 y 90 del REGLAMENTO DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO.

El prestador de servicio podrá modificar el número de cuenta y el nombre de la Institución bancaria, sin que sea necesario modificar el contrato, siempre que el representante legal dé aviso por escrito al Instituto FONACOT por lo menos con 10 (diez) días naturales de anticipación a la presentación de la factura.

21. NIVELES DE SERVICIO (SLA´s).

21.1 Tiempos de respuesta.

Los licitantes deberán considerar los siguientes tiempos para la atención y solución de las incidencias o problemas que se presenten durante la vigencia del contrato, por los servicios proporcionados.

	Atención y solución de las incidencias o problemas con base a su complejidad			
CONCEPTO	ALTA	MEDIA	BAJA	EXTREMA
Incidentes	* Menor a 04.00 horas	De 04.01 a 08.00 horas	De 08.01 horas a 12.00 horas	Se acuerda con la Subdirección General de Tecnologías de la Información y Comunicación.

CONCEPTO	Atención y solución de las incidencias o problemas con base a su complejidad			
	ALTA	MEDIA	BAJA	EXTREMA
Solicitudes	* Menor de 08.00 Horas	De 08.01 a 12.00 horas	De 12.01 horas a 16.00 horas	Se acuerda con la Subdirección General de Tecnologías de la Información y Comunicación.

* Horas hábiles

22. ENTREGABLES.

El licitante deberá considerar la generación de reportes para dar seguimiento a la operación de los servicios proporcionados al Instituto FONACOT; los reportes deberán entregarse a periodo vencido, dentro de los 05 días hábiles posteriores al cierre del periodo de que se trate.

Aquellos entregables que no sean presentados dentro del plazo señalado en el párrafo anterior serán considerados como no entregados y sujetos a penalizaciones o deducciones aplicables conforme a lo señalado en el capítulo correspondiente de este Anexo Técnico.

Entregables mensuales del proyecto:

- Reporte de incidentes por cada uno de los servicios
- Reporte de solicitudes por cada uno de los servicios
- Reporte de ciber inteligencia (reporte ejecutivo)
- Reporte de disponibilidad de cada uno de los servicios.
- Reporte de tableros de control.
- Reporte de análisis de vulnerabilidades**. (cada 6 meses o bajo demanda del Instituto FONACOT)**
- Reportes de Forenses**. (bajo demanda del Instituto FONACOT)**
  - SOW.
  - INFORME DE ANÁLISIS DE CÓMPUTO FORENSE – TÉCNICO.
  - MEMORIA TÉCNICA DE ADQUISICIÓN DE INFORMACIÓN.
- Reporte de cambios en la configuración de los servicios.
- Reporte de trazabilidad de SVI.
- Reporte de dependencia lógica de los servicios críticos.
- Reporte de afectaciones de activos.
- Reporte de implementación del Servicio de Gestión de Seguridad de la Información.

El licitante ganador deberá proporcionar los entregables relacionados en este apartado, para que sean revisados por el Administrador del Contrato o personal autorizado por el Instituto Fonacot, quien en su caso notificará y solicitará formalmente al licitante ganador realizar las correcciones que considere pertinentes a la documentación, previo acuerdo mutuo entre ambas partes. A la entrega de cada documento se deberá suscribir el acta de entrega-recepción correspondiente.

El Instituto FONACOT se reserva el derecho para solicitar reportes adicionales, las cuales se vinculen con el otorgamiento del servicio requerido en este Anexo Técnico.

23. PENAS CONVENCIONALES

En términos de lo previsto por los artículos 53 de La Ley, 95 y 96 de El Reglamento, el Instituto FONACOT, aplicará a EL LICITANTE en caso de resultar el licitante ganador penas convencionales a EL LICITANTE en caso de resultar el licitante ganador, de conformidad con lo siguiente:

PENAS CONVENCIONALES		
No.	Descripción	Monto
1	Minuta de la Reunión de Kick Off de este con el numeral 22. ENTREGABLES del Anexo Técnico.	1% del monto total mensual del mes en cuestión, por día natural de atraso en la entrega de la Minuta de la Reunión de Kick Off, debidamente firmada por los asistentes por parte de EL LICITANTE la cual deberá entregarse a más tardar a los cinco días hábiles de haberse llevado a cabo la referida reunión.
2	Atraso en la entrega del Plan de Trabajo General de conformidad con el numeral 22. ENTREGABLES del Anexo Técnico.	1% del monto total mensual del mes en cuestión, por día natural de atraso en la entrega del Plan de Trabajo General, el cual deberá entregarse a más tardar a los cinco días hábiles después de firmado el Contrato.
3	Atraso en la entrega del Plan de Trabajo Detallado por Servicio a Implementar, de acuerdo con las necesidades del servicio integral de conformidad con el numeral 22 ENTREGABLES del Anexo Técnico.	1% del monto total mensual del mes en cuestión, por día natural de atraso en la entrega de los Planes de Trabajo a Detalle para la implementación de cada servicio, dichos planes detallados deberán entregarse a más tardar a los diez días hábiles después de entregado el Plan de Trabajo General.
4	Memoria Técnica de cada Servicio Implementado de conformidad con el numeral 22 ENTREGABLES del Anexo Técnico.	1% del monto total mensual del mes en cuestión, por día natural de atraso en la entrega de la Memoria Técnica, la cual deberá entregarse a más tardar a los cinco días de concluido la implementación respectiva del servicio correspondiente.
5	Atraso en los tiempos establecidos en la implementación de los servicios objetos de conformidad con el numeral 22 ENTREGABLES del Anexo Técnico.	3% del monto total mensual del mes en cuestión, por día natural de atraso en la implementación de cada uno de los servicios objeto del presente, de acuerdo a su plan de trabajo detallado correspondiente.

24. DEDUCTIVAS.

De acuerdo con lo previsto por los artículos 53 BIS de La Ley y 97 de El Reglamento, el Instituto FONACOT aplicará al licitante ganador, deductivas de conformidad con lo siguiente:

DEDUCTIVAS		
No.	**Descripción**	**Monto**
1	Incumplimiento parcial o entrega mal realizada o incompleta en los niveles de servicio establecidos en el numeral **21. NIVELES DE SERVICIO (SLA´s).**	3% del monto total mensual del mes en cuestión, por incumplimiento parcial o entrega mal realizada o incompleta a los niveles de servicio.
2	Incumplimiento en la entrega total de cada uno de los servicios, ya sea por mala realización o entrega incompleta, de cualquiera de los servicios plasmados en el numeral **5. DESCRIPCIÓN GENERAL DEL SERVICIO.**	3% del monto total mensual del mes en cuestión, por incumplimiento en la entrega total de cada uno de los servicios, ya sea por mala realización o entrega incompleta, de cualquiera de los servicios plasmados, por más de 1 hora.

DEDUCTIVAS		
No.	**Descripción**	**Monto**
3	Incumplimiento en el tiempo de asignación o reemplazo de los recursos humanos, establecidos en el numeral **13. ADMINISTRACIÓN DE LOS SERVICIOS.**	1% del monto total mensual del mes en cuestión, por día natural por incumplimiento parcial o fuera de los tiempos establecidos para el reemplazo de los recursos humanos.
4	Incumplimiento parcial o entrega mal realizada o incompleta por cada uno de los entregables mensuales, establecidos en el numeral **22. ENTREGABLES.**	3% del monto total mensual del mes en cuestión, por día natural por incumplimiento parcial o entrega mal realizada o incompleta de cada uno de los entregables mensuales.

25. GARANTÍA DE CUMPLIMIENTO DE CONTRATO PLURIANUAL.

El licitante que resulte adjudicado deberá garantizar el fiel y exacto cumplimiento del contrato, mediante fianza expedida por institución autorizada legalmente para ello, conforme a lo que establecen los artículos 48 fracción II y 49 fracción II de la LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO y el artículo 87 del REGLAMENTO DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO, por el importe del 10% (Diez por ciento) del monto total por erogar en el ejercicio fiscal de que se trate, debiendo ser renovada cada ejercicio fiscal por el monto máximo a ejercer en el mismo, la cual deberá presentarse para el primer ejercicio fiscal a más tardar dentro de los diez días naturales posteriores a la firma del contrato y para los ejercicios subsecuentes deberá ser dentro de los primeros diez días naturales del ejercicio fiscal que corresponda. La renovación señalada deberá realizarse conforme a lo dispuesto por la fracción II y el último párrafo del artículo 103 del REGLAMENTO DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO, a favor del Instituto del Fondo Nacional para el Consumo de los Trabajadores, la cual deberá entregarse en la Dirección de Recursos Materiales y Servicios, cita en Avenida Insurgentes Sur No. 452, 1° Piso, Colonia Roma Sur, Delegación Cuauhtémoc, C.P. 06760., Ciudad de México.

- La fianza deberá redactarse en la forma y términos establecidos.
- La no entrega de la garantía es motivo de rescisión del contrato.

26. GARANTÍA DE RESPONSABILIDAD CIVIL

El licitante ganador se obliga a proporcionar al administrador del contrato por el pago de los daños que por causas imputables a la mano de obra de su personal pueda causar a los sistemas, equipos e instalaciones en general y los problemas de cualquier naturaleza que puedan derivar directamente de defectos o incumplimiento en la prestación de los servicios contratados y que no sean objeto de penalización, póliza expedida por institución autorizada por las Leyes Mexicanas a favor del Instituto del Fondo Nacional para el Consumo de los Trabajadores cuyo monto será de **$3,000,000.00** (Tres millones de pesos 00/100 M.N.), que garantice la protección de daños y perjuicios que pudieran presentarse como resultado de las actividades propias del licitante ganador por la ejecución de los servicios que se contraten derivados de este procedimiento. **La cual deberá ser entregada dentro de los 5 días hábiles posteriores al Acto de Fallo en la Dirección de Tecnologías de la Información sito en Avenida Insurgentes Sur No. 452, 2° Piso, Col. Roma Sur, C.P. 06760, Delegación Cuauhtémoc, Ciudad de México.**

Si por causa de la prestación del servicio se producen daños a los sistemas, equipos o componentes del mismo se hará valida la garantía por responsabilidad civil que el licitante ganador se obliga a presentar al Administrador del Contrato.

En caso de que algún siniestro supere el monto de la Póliza requerida, el licitante ganador se hará cargo de la totalidad de los gastos que este llegue a generar.

27. GARANTÍA DE RESPONSABILIDAD LABORAL.

Queda expresamente estipulado que el personal del licitante ganador estará bajo la responsabilidad directa del mismo, por lo tanto, en ningún momento se considerará a la Convocante como patrón sustituto, ni tampoco al licitante ganador como intermediario, por lo que el Instituto FONACOT, no tendrá relación alguna de carácter laboral con dicho personal y consecuentemente queda liberada de cualquier responsabilidad de las reclamaciones que se pudieran presentar en contra de la Convocante.

28. NORMAS APLICABLES.

Las normas aplicables a las que se debe hacer referencia como parte de la prestación del servicio son las siguientes:

Norma ISO/IEC 27001, certificación ISO 27001 y certificación del Foro de Respuesta a Incidentes y Equipos de Seguridad (FIRST).

29. CONFIDENCIALIDAD.

Con motivo de la prestación del servicio el Instituto FONACOT proporcionará al licitante ganador toda la información y documentación necesaria para el debido desempeño de sus funciones, misma que el licitante ganador se obliga a guardar y a hacer guardar estricta confidencialidad y reserva.

Toda la información que con motivo de la prestación del servicio objeto del contrato respectivo, el Instituto FONACOT entregue al licitante ganador, así como toda la información que el licitante ganador desarrolle, serán propiedad exclusiva del Instituto FONACOT, considerándose esta información como confidencial y privilegiada, por lo que estará protegida en todo momento como secreto industrial en términos de la Ley de la Propiedad Industrial, de la Ley Federal de Transparencia y Acceso a la Información Pública y de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, debiendo los licitantes ganadores, guardar la secrecía y confidencialidad sobre la misma, obligándose a no usarla, copiarla, transmitirla o divulgarla a terceros sin consentimiento expreso y por escrito del Instituto FONACOT.

Lo anterior debe entenderse, como que el licitante ganador se abstendrá de manera directa o indirecta de editar, divulgar, publicar, comercializar, usar y modificar total o parcialmente, la información proporcionada, conocida, desarrollada u obtenida, por cualquier medio, sin la debida autorización del Instituto FONACOT, respondiendo en caso contrario por los daños y perjuicios que se llegaran a ocasionar para ambas partes, en el entendido de que dichos actos podrán generar la rescisión del contrato. En caso de que la conducta desplegada por el licitante ganador sea constitutiva de delito, en perjuicio del Instituto FONACOT, ésta podrá hacer la denuncia correspondiente ante el ministerio público competente.

De la misma manera convienen en que la información confidencial a que se refiere esta cláusula puede estar contenida en documentos, fórmulas, cintas magnéticas, programas de computadora, CD o cualquier otro material que tenga información jurídica, operativa, técnica, financiera, de análisis, compilaciones, estudios, gráficas o cualquier otro similar.

30. ADMINISTRACIÓN DEL CONTRATO

El administrador del contrato será el titular de la **Subdireccion General de Tecnologias de la Información y Comunicación** quien será el responsable de supervisar, coordinar la prestación del servicio y de otorgar el visto bueno a las facturas del servicio devengado de acuerdo con lo descrito en este Anexo Técnico.

31. PLAN DE TRANSICIÓN AL CIERRE

El LICITANTE ganador desarrollará un plan de transición y takeover de los servicios inherentes de Seguridad de la Información, mismo que será sujeto a revisión por parte del Instituto FONACOT.

El plan de transición dará inicio 30 días naturales previos a la conclusión del contrato o de manera anticipada a través de una solicitud expresa del **Administrador del Contrato**, como parte del Plan de Transición el LICITANTE ganador deberá apoyar en las actividades necesarias para garantizar la continuidad operativa de los servicios de seguridad que se encuentran actualmente, ya sea para el Instituto FONACOT o para un nuevo prestador de servicio

El plan de transición deberá contener al menos los siguientes puntos de manera enunciativa más no limitativa:

- Memorias técnicas:
  - Listado de componentes tecnológicos y su hardware, software, licenciamiento que sean parte del servicio. (Cantidad, Marca, Modelo, Número de Serie, Ubicación del equipo o parte)
  - Documento que contenga la descripción del proceso de operación.
  - Documento que incluya el proceso de respaldo de información.
  - Documento que contenga el proceso de restauración de la información
  - Documento que contenga el proceso de monitoreo de los componentes.
  - Diagrama de Infraestructura que contenga la última configuración con la que se encuentra operando actualmente el Instituto.
  - Documento que contenga el listado de usuarios y privilegios de los componentes. (Este documento se entregará al administrador del proyecto por parte del instituto, el cual se entregará al licitante ganador en el momento que el instituto lo decida).
- Transferencia de Recursos:
  - Entregar los respaldos de las ultimas configuraciones en sus versiones finales autorizadas y operando en el instituto en un medio digital.
- Transferencia de Información:
  - Acompañamiento al licitante ganador en las mesas de trabajo de arranque del proyecto con el instituto.
  - Documento que incluya la información adicional solicitada por el licitante ganador y entregada al instituto como parte de las actividades de transición.

Autorizó

Mtro. Horacio Sánchez Tinoco
Subdirector General de Tecnologías de la Información y Comunicación

Elaboró

Lic. Gerardo Daza López
Encargado de las funciones de Oficial de Seguridad de la Información en el Instituto FONACOT

ANEXO II
COTIZACIÓN

Ciudad de México a 19 de julio de 2022
Asunto: Se acepta la formalización
de un nuevo contrato

Mtro. Horacio Sánchez Tinoco
Subdirector General de Tecnologías de la Información y Comunicación del Instituto del Fondo Nacional para el Consumo de los Trabajadores
P r e s e n t e.

El suscrito Allan Morgan Velasco, en mi calidad de representante legal de **IQSEC, S.A. de C.V.** personalidad acreditada mediante escrito que presente de fecha 18 de julio de 2022), y en atención a su oficio número **SGTIC.361.07.2022** de fecha **13 de julio de 2022**, referente a su solicitud para la suscripción de un nuevo contrato para la prestación del "Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones", al respecto manifiesto lo siguiente:

Que por medio de la presente **manifiesto el consentimiento de mi representada para suscribir el nuevo contrato referido,** con iguales condiciones al contrato número I-SD-2018-114, mismo que también fue suscrito entre ese Instituto y mi representada en cuanto a precio, características y calidad de los bienes o servicios, motivo por el cual **anexo a la presente la cotización requerida** de los servicios por el periodo del 16 de agosto de 2022 al 31 de diciembre de 2022.

Sin otro particular por el momento, aprovecho la oportunidad para enviarle un cordial saludo y quedo atento a respuesta.

TRABAJO

RECIBIDO
20 JUL 2022
SUBDIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

ATENTAMENTE

ALLAN MORGAN VELASCO
REPRESENTANTE LEGAL
DE IQSEC S.A. DE C.V.

Ciudad de México a 19 de julio de 2022
Asunto: Se remite propuesta económica

Mtro. Horacio Sánchez Tinoco
Subdirector General de Tecnologías de la Información y Comunicación del Instituto del Fondo Nacional para el Consumo de los Trabajadores
P r e s e n t e.

El que suscribe Allan Morgan Velasco en mi carácter de Representante Legal de la empresa **IQSEC, S.A. de C.V.**, en atención a su oficio número oficio número **SGTIC.361.07.2022** de fecha **13 de julio de 2022,** referente a su solicitud para la suscripción de un nuevo contrato para la prestación del "Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones", por medio del presente, adjunto se servirá encontrar la **Propuesta Económica** que **IQSEC, S.A. de C.V.** pone a su disposición:

Núm.	Servicio	Precio Unitario Mensual	IVA	Monto Total
1	Servicio de gestión, seguimiento y control de incidentes	$ 453,527.30	$ 72,564.37	$ 526,091.67
2	Servicio de validación de identidad	$ 491,613.10	$ 78,658.10	$ 570,271.20
3	Servicio de detección e investigación de vulnerabilidades y pruebas de penetración	$ 399,244.11	$ 63,879.06	$ 463,123.17
4	Servicio de control y gestión de usuarios	$ 415,879.29	$ 66,540.69	$ 482,419.98
5	Servicio de protección de bases de datos	$ 483,613.99	$ 77,378.24	$ 560,992.22
6	Servicio de administración del MGSI	$ 513,590.78	$ 82,174.52	$ 595,765.30
TOTAL		**$ 2,757,468.56**	**$ 441,194.97**	**$ 3,198,663.54**

Sin más por el momento, reciba un cordial saludo, quedando de ustedes muy atentos para cualquier duda, comentario o complemento a la información enviada.

ATENTAMENTE

ALLAN MORGAN VELASCO
REPRESENTANTE LEGAL
DE IQSEC S.A. DE C.V.

TRABAJO

RECIBIDO
20 JUL 2022
SUBDIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

ACTA DE LA VIII SESIÓN ORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES

En la Ciudad de México a 9 de noviembre del 2022, Ilse Campos Loera, Secretaria Técnica del Comité de Transparencia del Instituto del Fondo Nacional para el Consumo de los Trabajadores, en adelante Instituto FONACOT, hizo constar que, con fundamento en las Reglas de Integración y Funcionamiento del Comité de Transparencia, se llevó a cabo la Octava Sesión Ordinaria 2022 a través de medios electrónicos, mediante la Plataforma Tecnológica Teams, misma que se desahogó de la siguiente forma:

Para iniciar la Sesión, la Secretaria Técnica solicitó a los Miembros del Comité de Transparencia, en adelante los Miembros, manifestar su asistencia para estar en posibilidad de continuar con el desarrollo de la misma.

A las 13:30 horas, la Secretaria Técnica verificó el ingreso de los Miembros a la videoconferencia llevada a cabo mediante la Plataforma Tecnología Teams, por lo que solicitó permiso a Erick Morgado Rodríguez, Presidente del Comité de Transparencia, para llevar a cabo la lectura de la lista de asistencia, haciendo constar que, en la Sesión se encontraron los siguientes integrantes:

Nombre	Puesto en el Instituto FONACOT
Erick Morgado Rodríguez	Presidente del Comité de Transparencia Abogado General
Erika Helena Psihas Valdés	Responsable del Área Coordinadora de Archivos Directora de Recursos Materiales y Servicios Generales
Lidio Ruiz García	Suplente de la Titular del Órgano Interno de Control en el Instituto FONACOT, de conformidad con el oficio No. OIC/TOIC/14/120/2022/125 de fecha 12 de abril de 2022 Titular del Área de Responsabilidades
Miguel Ángel López Reyes	Jefe de Oficina de Integración Presupuestal

Con base en lo anterior, la Secretaria Técnica informó la existencia del Quórum Legal para la celebración de la Sesión e informó que la misma se grabaría para realizar el acta correspondiente, la cual será resguardada por la Unidad de Transparencia en el entendido de que los participantes tienen autorización para conocer el contenido de lo grabado a través de los medios en que se dio el consentimiento, salvo casos excepcionales previstos en la Ley.

Por lo anterior, se sometió a consideración de los Miembros el Orden del Día de la presente Sesión.

II. Aprobación del Orden del Día

I. LISTA DE ASISTENCIA Y VERIFICACIÓN DEL QUÓRUM LEGAL.

II. LECTURA Y APROBACIÓN DEL ORDEN DEL DÍA.

III. LECTURA Y APROBACIÓN DEL ACTA CORRESPONDIENTE A LA 7ª SESIÓN ORDINARIA DE FECHA 12 DE OCTUBRE DE 2022.

IV. INFORME Y SEGUIMIENTO DEL ACUERDO DE LA 4ª SESIÓN EXTRAORDINARIA DEL COMITÉ DE TRANSPARENCIA.

V. PRESENTACIÓN DE LOS ASUNTOS QUE SE SOMETIERON A CONSIDERACIÓN DEL COMITÉ DE TRANSPARENCIA.

1. La Dirección de Integración y Control Presupuestal solicita la clasificación de la información con carácter confidencial de la versión pública de **540** facturas de viáticos, presentadas con la finalidad de dar cumplimiento a las Obligaciones de Transparencia, establecidas en el Artículo 70 fracción IX de la Ley General de Transparencia y Acceso a la Información Pública.

2. La Dirección de Recursos Materiales y Servicios Generales solicita la clasificación de la información con carácter confidencial de la versión pública de **119** contratos, **11** pedidos, **09** convenios

modificatorios y **01** justificación, presentados con la finalidad de dar cumplimiento a las Obligaciones de Transparencia, establecidas en el Artículo 70 fracción XXVII y XXVIII de la Ley General de Transparencia y Acceso a la Información Pública.

VI. ASUNTOS GENERALES.

1. La Secretaria Técnica presentó como Toma de Conocimiento, las Resoluciones de las Denuncias por incumplimiento a las Obligaciones de Transparencia emitidas por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

La Secretaria Técnica solicitó a los Miembros emitieran su voto para la aprobación del Orden del Día:

Nombre de los Miembros del Comité de Transparencia	Sentido de los votos	
	A favor	En contra
Erick Morgado Rodríguez Presidente del Comité	✓	
Erika Helena Psihas Valdés Responsable del Área Coordinadora de Archivos	✓	
Lidio Ruiz García Suplente de la Titular del Órgano Interno de Control en el Instituto FONACOT, de conformidad con el oficio No. OIC/TOIC/14/120/2022/125 de fecha 12 de abril de 2022	✓	

Por lo que una vez expresada la votación, se adoptó el siguiente Acuerdo:

CT8SO.09.11.2022-II
El Comité de Transparencia del Instituto del Fondo Nacional para el Consumo de los Trabajadores, confirma con 3 votos a favor y ninguno en contra la aprobación del Orden del Día de la 8ª Sesión Ordinaria.

III. Lectura y aprobación del Acta correspondiente a la 7ª Sesión Ordinaria de fecha 12 de octubre de 2022.

Derivado de la revisión del Acta, se solicitó a los Miembros informaran si tenían algún comentario u observación al respecto, al no haber comentarios, solicitó el sentido de su voto:

Nombre de los Miembros del Comité de Transparencia	Sentido de los votos	
	A favor	En contra
Erick Morgado Rodríguez Presidente del Comité	✓	
Erika Helena Psihas Valdés Responsable del Área Coordinadora de Archivos	✓	
Lidio Ruiz García Suplente de la Titular del Órgano Interno de Control en el Instituto FONACOT, de conformidad con el oficio No. OIC/TOIC/14/120/2022/125 de fecha 12 de abril de 2022	✓	

Por lo que una vez expresada la votación, se adoptó el siguiente Acuerdo:

CT8SO.09.11.2022-III
El Comité de Transparencia del Instituto del Fondo Nacional para el Consumo de los Trabajadores, confirma con 3 votos a favor y ninguno en contra el Acta correspondiente a la 7ª Sesión Ordinaria de fecha 12 de octubre de 2022.

IV. Informe y Seguimiento del Acuerdo de la 4ª Sesión Extraordinaria del Comité de Transparencia

La Secretaria Técnica informó que en la 7ª Sesión Ordinaria que aún no se cuenta con la respuesta del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en relación a la consulta respecto del testado del domicilio de la persona moral; sin embargo, se hizo del conocimiento que se mandó Oficio de consulta y a la fecha no contamos con respuesta por parte de ese Instituto.

Derivado de lo anterior, se solicitó a los Miembros informaran si tenían algún comentario u observación al respecto, al no haber comentarios, se procedió a la lectura del siguiente punto del Orden del Día.

V. Presentación de los asuntos que se sometieron a consideración del Comité de Transparencia

1. La Dirección de Integración y Control Presupuestal solicitó la clasificación de la información con carácter confidencial de la versión pública de **540** facturas de viáticos, presentadas con la finalidad de dar cumplimiento a las Obligaciones de Transparencia, establecidas en el Artículo 70 fracción IX de la Ley General de Transparencia y Acceso a la Información Pública.

Con la finalidad de dar cumplimiento a las Obligaciones de Transparencia, establecidas en el artículo 70 fracción IX de la Ley General de Transparencia y Acceso a la Información Pública, esa Dirección solicitó la clasificación de información de **540** facturas de viáticos testando el domicilio, código QR, RFC, folio fiscal, correo electrónico particular, sello digital del SAT, número de serie del emisor, nombre, número del CSD, cadena original del complemento de certificación digital del SAT, nombre de terceros, cuenta y clabe interbancaria y sello digital del emisor o CFDI de acuerdo a la siguiente:

Fundamentación

Artículo 116 de la Ley General de Transparencia y Acceso a la Información Pública; artículo 113 fracciones I y III de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Lineamiento Trigésimo Octavo fracciones I y II de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.

Motivación

Por corresponder a datos que identifican o hacen identificable a la persona y por corresponder a hechos y actos de carácter económico, contable o administrativos, relativos a una persona.

La Secretaria Técnica, solicitó el sentido de su voto ya que no existieron comentarios al respecto:

Nombre de los Miembros del Comité de Transparencia	Sentido de los votos	
	A favor	En contra
Erick Morgado Rodríguez Presidente del Comité	✓	
Erika Helena Psihas Valdés Responsable del Área Coordinadora de Archivos	✓	
Lidio Ruiz García Suplente de la Titular del Órgano Interno de Control en el Instituto FONACOT, de conformidad con el oficio No. OIC/TOIC/14/120/2022/125 de fecha 12 de abril de 2022	✓	

Derivado de lo anterior, los Miembros adoptaron el siguiente Acuerdo:

CT8SO.09.11.2022-V.1
El Comité de Transparencia del Instituto del Fondo Nacional para el Consumo de los Trabajadores, con fundamento en los artículos 44 fracción II; 103; 106 fracción III; 116 y 137 de la Ley General de Transparencia y Acceso a la Información Pública; Artículos 65 fracción II; 98 fracción III; 102; 113 fracciones I y III y 140 de la Ley

Federal de Transparencia y Acceso a la Información Pública y los Lineamientos Séptimo fracción III; Noveno y Trigésimo Octavo fracciones I y II de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas, confirma con 3 votos a favor y ninguno en contra la clasificación de información con carácter Confidencial de la versión pública de **540** facturas de viáticos, presentados con la finalidad de dar cumplimiento a las Obligaciones de Transparencia, establecidas en el Artículo 70 fracción IX de la Ley General de Transparencia y Acceso a la Información Pública.

2. La Dirección de Recursos Materiales y Servicios Generales solicitó la clasificación de información con carácter confidencial de la versión pública de **119** contratos, **11** pedidos, **09** convenios modificatorios y **01** justificación, presentados con la finalidad de dar cumplimiento a las Obligaciones de Transparencia, establecidas en el artículo 70 fracción XXVII y XXVIII de la Ley General de Transparencia y Acceso a la Información Pública.

Con la finalidad de dar cumplimiento a las Obligaciones de Transparencia, establecidas en el artículo 70 fracción XXVII y XXVIII de la Ley General de Transparencia y Acceso a la Información Pública, esa Dirección solicitó la clasificación de información de **119** contratos, **11** pedidos, **9** convenios modificatorios y **01** justificación testando el OCR o número identificador, número telefónico, correo electrónico, número de cuenta y clabe, clave de identificación de la credencial (CIC), domicilio, nombre de terceras personas, clave de elector, número de pasaporte y clave catastral de acuerdo a la siguiente:

Fundamentación

Artículo 116 de la Ley General de Transparencia y Acceso a la Información Pública; artículo 113 fracciones I y III de la Ley Federal de Transparencia y Acceso a la Información Pública; artículo 3 fracción IX de la Ley General de Datos Personales en Posesión de Sujetos Obligados, así como el Lineamiento Trigésimo Octavo fracciones I y II de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.

Motivación

Por corresponder a datos que identifican o hacen identificable a la persona y por corresponder a hechos y actos de carácter económico, contable o administrativos, relativos a una persona.

La Secretaria Técnica preguntó a los Miembros si tenían algún comentario u observación sobre el asunto:

El Suplente de la Titular del Órgano Interno de Control, hizo referencia a los 119 contratos y señaló que en 26 corresponden a contratos de arrendamiento, y derivado a que no se celebra por la Ley de Adquisiciones

consideró que el RFC debería testarse; así mismo mencionó que se debió hacer la distinción de cuáles son los que se refieren a la fracción XXVII y cuáles a la fracción XXVIII.

La Secretaria Técnica hizo del conocimiento que en futuras sesiones se hará la distinción solicitada por el Suplente de la Titular del Órgano Interno de Control a que hizo referencia el Suplente de la Titular del Órgano Interno de Control y señaló que el RFC se deja libre en los 26 contratos de referencia ya que se celebran por la Ley General de Bienes Nacionales y están relacionados con la fracción XXXII del artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública.

La Responsable del Área Coordinadora de Archivos, manifestó lo mismo del porqué se dejó sin testar el RFC de esos contratos, mencionando que son proveedores.

Nombre de los Miembros del Comité de Transparencia	Sentido de los votos	
	A favor	En contra
Erick Morgado Rodríguez Presidente del Comité	✓	
Erika Helena Psihas Valdés	✓	

Responsable del Área Coordinadora de Archivos		
Lidio Ruiz García Suplente de la Titular del Órgano Interno de Control en el Instituto FONACOT, de conformidad con el oficio No. OIC/TOIC/14/120/2022/125 de fecha 12 de abril de 2022		

Derivado de lo anterior, los Miembros adoptaron el siguiente Acuerdo:

CT8SO.09.11.2022-V.2
El Comité de Transparencia del Instituto del Fondo Nacional para el Consumo de los Trabajadores, con fundamento en los artículos 44 fracción II; 103; 106 fracción III; 116 y 137 de la Ley General de Transparencia y Acceso a la Información Pública; Artículos 65 fracción II; 98 fracción III; 102; 113 fracciones I y III y 140 de la Ley Federal de Transparencia y Acceso a la Información Pública y los Lineamientos Séptimo fracción III; Noveno y Trigésimo Octavo fracciones I y II de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas, confirma con 2 votos a favor y una abstención, la clasificación de información con carácter Confidencial de la versión pública de **119** contratos, **11** pedidos, **09** convenios modificatorios y **01** justificación, presentados con la finalidad de dar cumplimiento a las Obligaciones de Transparencia, establecidas en el artículo 70 fracción XXVII y XXVIII de la Ley General de Transparencia y Acceso a la Información Pública.

La Secretaria Técnica, señaló que se concluyeron los asuntos presentados para su confirmación.

VI. Asuntos Generales

1. La Secretaria Técnica presentó como Toma de Conocimiento, las Resoluciones de las Denuncias por incumplimiento a las Obligaciones de Transparencia emitidas por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Denuncia	Sujeto Obligado	Fracción
DIT 0592/2022	Tribunal Federal de Justicia Administrativa	XIX "Servicios que ofrecen"
DIT 0593/2022	Tribunal Federal de Justicia Administrativa	XXIX "Informes que se generen"
DIT 0751/2022	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales	IX "Facturas de viáticos"

Por último, no habiendo más asuntos que tratar y siendo las 13 horas con 47 minutos, se da por terminada la Octava Sesión Ordinaria 2022 del Comité de Trasparencia.

Erick Morgado Rodríguez
Abogado General
Presidente del Comité de Transparencia

Erika Helena Psihas Valdés
Directora de Recursos Materiales y Servicios Generales
Responsable del Área Coordinadora de Archivos

Lidio Ruiz García
Titular del Área de Responsabilidades
Suplente de la Titular del Órgano Interno de Control